PhD-FSTM-2020-40
The Faculty of Sciences, Technology and Medicine

DISSERTATION

Defence held on 20/07/2020 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Nida KHAN

BLOCKCHAIN-ENABLED TRACEABILITY AND IMMUTABILITY FOR FINANCIAL APPLICATIONS

Dissertation defence committee

Dr Radu State, dissertation supervisor
Professor, Université du Luxembourg

Dr Lehnert Thorsten, Chairman
Professor, Université du Luxembourg

Dr Abdelkader Lahmadi, Vice Chairman
Professor, Université de Lorraine

Dr Zsofia Kräussl
Postdoctoral researcher, Université du Luxembourg

Dr Omar Cherkaoui
Professor, Université du Québec à Montréal

Dissertation supervisor: Dr. Radu State Nida Khan

Blockchain-enabled Traceability and Immutability for Financial Applications

Abstract

Blockchain is an emerging, foundational, disruptive technology with the potential to completely overhaul the existing financial infrastructure. The finance sector is leading in the deployment of blockchain to resolve endemic issues related to transparency, third-party fraud as well as time-consuming and expensive transactions. The finance sector has not been able to serve the underbanked and unbanked populations of the world so far. COVID-19 in 2020 has indicated that a strong digital infrastructure is needed to be able to deal better with disruption and blockchain can play a pivotal role in establishing this digital infrastructure. The dissertation explores the efficacy of exploiting the transparency and immutability characteristics of blockchain platforms in a financial ecosystem.

The dissertation elaborates on blockchain technology employing a succinct approach, which serves as the foundation to comprehend the contributions of the present research work. Blockchain governance is an unresolved facet of the technology, in the absence of which, the distributed network can fail to function optimally or even stall. The dissertation gives a verified mathematical model, derived using Nash equilibrium, to function as a framework for blockchain governance. The usage of blockchain in financial organizations entails the requirement of a sound management strategy to obfuscate the complexities of the technology and replicate the administrative functions existing in legacy systems. The research work elucidates the design, implementation and evaluation of a management plane to monitor and manage blockchain-based decentralized applications. Privacy of financial data is extremely important for any financial organization but blockchain, by virtue of its inherent infrastructure, poses a challenge in this respect. This is also one of the overarching factors that makes usage of blockchain questionable from the European GDPR perspective. Privacy-preserving blockchain platforms have also proved to be vulnerable to data breaches. The dissertation solves this problem by the development and evaluation of a management plane for differential privacy preservation through smart contracts. The research work discusses the compliance of the privacy management plane to GDPR using a permissioned blockchain platform.

The new economic paradigm enforced by blockchain, decentralized finance, presents novel challenges and unprecedented strategic advantages. The dissertation is a pioneer in conducting an implementation-based, comparative and an exploratory analysis of tokenization of ethical investment certificates. Social finance markets have been developing in Europe and are viewed as sustainable finance by the European Commission. The research work verifies the utility of blockchain to solve some prevalent issues in social finance. The work accomplishes this through the development and testing of a blockchain-based donation application. A qualitative review of the economic impact of blockchain-based micropayments has also been conducted. The discussion on the economic impact also includes a proposition for extending the access of blockchain-based financial services to the underbanked and unbanked people.

The work concludes with a hypothetical model of a financial ecosystem, depicting the deployment of the major contributions of this dissertation.

Contents

List of figures

List of tables

List of Algorithms

For my husband, Tabrez, and children, Umar, Khalid and Saad.

Acknowledgments

Our existence on this planet is dependent on the support and guidance we get from others and no human has ever achieved anything noteworthy in the absence of the aforementioned. I would like to thank my dissertation supervisor, Dr. Radu State, who not only encouraged independent thinking but also motivated many novel scientific thoughts, which were later transformed into pioneering practical implementations. His emphasis on not just the intellectual development from a research perspective, but overall honing of the personality contributed immensely to the person I am today. His guidance and teachings have left an indelible mark in my life, which will have a reflection in all the future work I do.

This research work was initiated and funded by the industrial partners, Anass Patel and Rachid Ouaich. I would like to thank both of them for believing in my potential to achieve the research goals of their fintech startup and giving me this opportunity to grow intellectually as a computer scientist. I would also like to thank them for making efforts to further my career in the corporate world by initiating many opportunities for me, whereby I could present my research to C-level executives and senior management of financial organizations.

This research work is the recipient of the prestigious *Luxembourg National Research Fund (FNR)* grant, (FnR project: FNR11617092)[1], accorded by the government of Luxembourg for innovative industrial projects. I would like to thank FNR for their support to further scientific research in Luxembourg.

I am obliged to Dr. Zsofia Kräussl, who infused the much needed expertise in finance, that was pivotal for the work I accomplished in this dissertation. I remain obliged to Dr. Abdelkader Lahmadi, who has played a very important role in strengthening my knowledge as a computer scientist. His kind approach to motivating new ideas can propel many innovative research outcomes.

[1] Luxembourg National Research Fund. (2017). AFR-PPP: Results 2017-1 Call. https://www.fnr.lu/afr-ppp-results-2017-1-call/, accessed May 15, 2020.

The support of the family is crucial to achieve success in any undertaking. The present work reached its culmination only because of my husband, Tabrez. I would like to thank him and my kids, to whom I have dedicated this work, for their unfaltering support and understanding of my passion. If it was not for their cooperation, this dissertation would have remained a dream. I would also like to thank my parents, Waseem and Anjum, who raised me cultivating in me a love for learning. This thought is further championed by my husband, which helped to not disrupt my journey of accumulation of knowledge. I would like to thank my brother, Abdur Rahman and his family, for their advice and support during this period. I would also like to thank my sister, Sana, who supported me like a steady rock in my decision to pursue research.

Special thanks to Sofiane for his support during the conceptual layout of the dissertation. Last but not the least, I would like to express my gratitude to all my co-authors, colleagues, friends and well-wishers, who helped to make this dissertation a reality.

"The computing scientist's main challenge is not to get confused by the complexities of his own making."

Edsger W. Dijkstra

1 Introduction

Blockchain is classified as a pillar of the Fourth Industrial Revolution that builds up on the erstwhile Digital Revolution. The emerging nascent technology, an immutable distributed database, is heralded as the most disruptive innovation [1] of recent times with the possibility to completely overhaul the existing economic system and social order [117]. Statistics forecast that the revenue generation from the blockchain industry would be equivalent to over $23.3 billion by 2023 from $2.2 billion in 2019 [2]. The expected massive growth, the envisaged disruptive nature of the technology and the inception of an entirely novel economic dimension by way of cryptoeconomics [47] has managed to garner both research and academic interest. Blockchain technology

[1] Pollock, D. (2018). The fourth industrial revolution built on blockchain and advanced with AI. https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-blockchain-and-advanced-with-ai/#7a756b94242b, accessed September 15, 2019.

[2] Statista. (2019). Size of the blockchain technology market worldwide from 2018 to 2023. https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/, accessed September 7, 2019

finds applications in diverse domains ranging from e-commerce for traceability of shipped physical assets [80, 169] to solutions catering to monetization of data exchanges between IoT devices [176]. IoT is predicted to be the single greatest source of data in the coming years [74] and the synergy between blockchain being used as a database to ensure non-repudiation of IoT data is a subject of ongoing research [101]. Mobile telecommunications using 5G can leverage upon blockchain technology to enable novel business models and services [29] while blockchain can also be employed to empower artificial intelligence [170]. The healthcare industry too can benefit from the incorporation of blockchain in the domain [2]. COVID-19 in 2020 has indicated that a strong digital infrastructure is needed to be able to deal better with disruption [3]. Blockchain can play a pivotal role in establishing this digital infrastructure as corroborated by a recent report by IBM highlighting the need for trusted data in the global marketplace, where it explores the power of blockchain to realize the goal of trusted, global interconnectedness [150].

Bitcoin, the first blockchain platform, came into inception in 2008 [138] followed by Ethereum in 2015 [197]. Numerous other blockchain platforms followed to diversify the services offered and initiate research in multiple domains, in particular the finance industry. The major proponent of blockchain, that has resulted in the growing popularity and potential prediction of complete overhauling of the financial ecosystem through its employment, is the dissolution of the need of an intermediary to transfer assets. This results in cost reductions while enabling real time financial transactions. Another distinguishing feature of blockchain networks that has established it in the forefront is the psychological satiation of power that the users experience when utilizing the technology. Blockchain, as a decentralized distributed database managed by a peer-to-peer network [178], transfers power from an organization/ single entity to the users of the technology, namely the common man. Blockchain is a kind of distributed ledger, where transactions are stored immutably using cryptography [157]. All blockchain platforms are distributed ledgers but not all distributed ledgers are blockchains as they might not have the underlying data structure present in blockchain platforms. The data in blockchain is organized into blocks, linked to each other through cryptography with the hash of the previous block, contributing to the data of the next block for hash generation. The cryptographic immutabil-

[3] Southworth, C. (2020). International Chamber of Commerce, UK [150].

ity guarantees non-repudiation of data, while the blocks of data chained together provide the ability to trace the entire path of the transaction taking place through a blockchain network. This enhances transparency, increases the trust, the users of the network place in the system, as well as facilitates ease of auditability.

The inception of blockchain catapulted the development of innovative use cases utilizing the trustless, decentralized environment, empowered by cryptocurrencies. The technology finds diverse applications in the finance sector like capital markets [50], escrow accounts [110], lending [83, 127], cryptocurrency wallets, insurance [67] and payment systems. Smart contracts, an application of blockchain, has reinvented the adherence to contractual clauses in financial applications [41]. Once the vulnerabilities [172] are dealt with, it can prove to be a strong tool in a nation's digital infrastructure.

1.1 Problem Statement

The focus of the present research is a study on the efficacy of deploying blockchain in financial applications and the traceability resulting thereon. The work highlights the benefits of blockchain-induced data immutability in financial applications. The immutability characteristic of blockchain, while advantageous, also poses challenges for compliance to the European General Data Protection Regulation (GDPR) [60], in the absence of which deployment of blockchain-based financial applications will remain questionable in the European Union. The research work proposes a circumvention to thwart the immutability of blockchain so that blockchain-based financial applications can adhere to GDPR. The research also conducts cost analyses of blockchain-enabled financial applications and delves into building basic management portals required for an effective deployment of blockchain-based financial applications in organizations.

The research work intends to answer the following research questions:

1. What governance strategy should be employed by a financial organization to ensure that blockchain-based financial products and services are available without any bottlenecks ?

2. What kind of management would be needed to integrate smart contracts in a financial organi-

zation ?

3. The European data protection law enforces compliance to GDPR. Would an organization, utilizing a blockchain-based application, be able to comply with this regulation ?

4. How does the new economic paradigm enforced by blockchain, decentralized finance (DeFi), compare with conventional finance ?

5. Social finance markets have been developing in Europe and are viewed as sustainable finance by the European Commission. Can blockchain be used for traceability to solve some endemic problems in social finance ?

1.2 Research Framework

The research framework involved an industrial fellowship coupled with academic research, which required a devotion of 40% of the research time to achieving research goals of the industrial partner. The remaining 60% of the time was utilized for academic research and a strategy was used whereby, we extended the research goals of the industry into academic research. We found the pertinent issues being faced in the industry and catered to framing our research questions around it to streamline academic work that was utilizable in the industry. The present research work is the recipient of the prestigious *Luxembourg National Research Fund* grant given by the government of Luxembourg for innovative industrial projects, post evaluation of the submitted research proposal by a national-level scientific body. The work is an attempt to solve some of the blockchain-based industrial issues through academic research. We sought to solve pertinent issues by developing blockchain-based industrial applications and exposing the solutions to tests and cost-benefit analyses to reach a conclusion on their efficacy for real world deployment. The research undertook a holistic approach, whereby we dealt not only with an analysis of the efficacy of deploying blockchain-based financial applications but also focused on the overall organizational ecosystem requirements that would provide a fertile ground for the applications to function optimally. The present work seeks to answer the research questions raised in Section 1.1 as follows:

1. **What governance strategy should be employed by a financial organization to ensure that blockchain-based financial products and services are available without any bottlenecks ?** Blockchain is a relatively nascent technology and the usage is complex for users outside the technology domain. The technology needs a governance framework to ensure its smooth functioning within any organization without impeding it's functioning. It is predicted that an absence of an apt governance mechanism can stall and result in a sub-optimized blockchain network [63], leading to frequent soft and hard forks in the network. A review of existing academic literature indicates that this is still a subject of ongoing research. The dissertation answers the research question in Chapter 3. The chapter proposes novel mathematical formulae usable to predict the best governance strategy that minimizes the occurrence of a hard fork as well as predicts the behavior of the majority during protocol updates.

2. **What kind of management would be needed to integrate smart contracts in a financial organization ?** A financial organization is organized into different departments like accounting, auditing, cash and credit amongst others. The organization is centrally controlled and to ensure integration of blockchain-based financial application with the existing legacy systems, our approach was to replicate the central administrative approach by providing a management plane to manage multiple smart contracts, deployed in a blockchain, by different departments of a financial organization. The dissertation answers the research question in Chapter 4. In this chapter, we propose a novel system to enable management operations in smart contracts and monitoring of blockchain-based applications. We design, implement and evaluate this novel system, which facilitates the integration of these operations through dedicated 'managing' smart contracts. We also build a monitoring tool to display public blockchain data using a dashboard coupled with a notification mechanism of any changes in private data to the administrator of the monitored decentralized application.

3. **The European data protection law enforces compliance to GDPR. Would an organization, utilizing a blockchain-based application, be able to comply with this regulation ?** Data privacy is of vital importance in financial organizations as a data breach can have legal, social and economic implications affecting the overall performance of an organization [98]. We review privacy-preserving blockchains in Chapter 5, Unit I to evaluate if they are suitable to ensure data privacy in blockchain-based applications. In Unit II of Chapter 5, we focus on the design, development and testing of a

novel privacy management plane utilizing differential privacy. We discuss the compliance of our implementation with respect to GDPR. GDPR dictates a completely new business model to be followed by technology companies [87] and our privacy management plane can serve as the prototype towards developing such a GDPR-compliant business model.

4. **How does the new economic paradigm enforced by blockchain, decentralized finance (DeFi), compare with conventional finance ?** Blockchain facilitates decentralized financial services, which are promised to be borderless, interoperable, transparent and innovative [35]. DeFi would initiate a novel mechanism to design financial regulation [203] but a precursor to this RegTech would be the analysis of some decentralized financial services in the view of their parallel implementation in conventional finance. We sought to answer this research question in Chapter 6 by tokenizing ethical investment certificates on Ethereum and conducting a cost-benefit analysis of the same when compared to issuance of analogous investment certificates. We coded a smart contract to facilitate tokenization and analyzed the feasibility of the approach for deployment in financial organizations. This research work was also instigated by the need of the industrial partner to tokenize ethical investment certificates, Sukuk. Luxembourg is one of Europe's primary listing avenues for Sukuk and provides access to a global investor base.

5. **Social finance markets have been developing in Europe and are viewed as sustainable finance by the European Commission. Can blockchain be used for traceability to solve some endemic problems in social finance ?** Social finance is viewed as a remedy for unemployment, poverty and inequality. Social finance steers the economy towards business models that cater to both social and environmental goals, namely the *Sustainable Development Goals (SDGs)* [4], as well as profit maximization, if envisaged, in organizations. Social financing and social banking have sprung up to target societal challenges in Europe post the economic crises of 2007 [78]. The dissertation answers the research question in Chapter 7, where we designed, developed and tested a blockchain-based donation application on Ethereum. We focused on one stakeholder group in social finance, namely charities on the demand side and individuals (donors) on the supply side as demarcated by the European Com-

[4] United Nations. Sustainable Development Goals. `https://sustainabledevelopment.un.org/?menu=1300`, accessed May 11, 2020.

mission's guide to designing and implementing initiatives for social finance instruments and markets [189]. Our use case was inspired by the industrial partners need for a donation platform based on crowdfunding for ethical projects. We highlight how some of the endemic problems are resolved by our developed decentralized donation application. Chapter 8 of the dissertation also seeks to answer this research question by conducting research on blockchain-based micropayments. Unit I of the chapter discusses the economic impact of blockchain-based micropayments, while highlighting the impact on the cybercrime economy. Unit II and Unit III of the chapter conduct a case study on Stellar and Lightning Network respectively.

The rest of the dissertation is organized as follows. State of the art including relevant background is given in Chapter 2. Conclusion, which involves a critical assessment of the research work in this dissertation and proposition for future work, is given in Chapter 9.

Figure 1.1 gives a graphical layout of the dissertation, demarcated according to the primary computer science concepts used in the chapters, while listing the research questions being targeted. Chapter 3 of the thesis deals with the concepts of game theory and utilizes Nash equilibrium to propose mathematical formulate for the selection of a Pareto optimal strategy for blockchain governance. Chapters 4, 5 and 6 deal with the utilization of blockchain-based smart contracts to design a management plane for financial organizations, achieve a GDPR-compliant usage of blockchain and motivate cost reductions by tokenization of ethical investment certificates respectively. Chapter 7 deals with the employment of a smart contract to implement the blockchain-based donation application as well as cryptocurrency to facilitate donations in micropayments. Chapter 8 deals with blockchain-based micropayments facilitated by the possibility of infinitesimal denominations of cryptocurrencies.

1.3 Contribution to Academic Literature

The present research work contributed to 9 first author publications and 4 co-author publications to steer the scientific progress of the society towards an enhanced understanding of the use of blockchain. Publication 3, [107] got the ***best workshop award*** at the 16th ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2019. The list of publications are as follows:

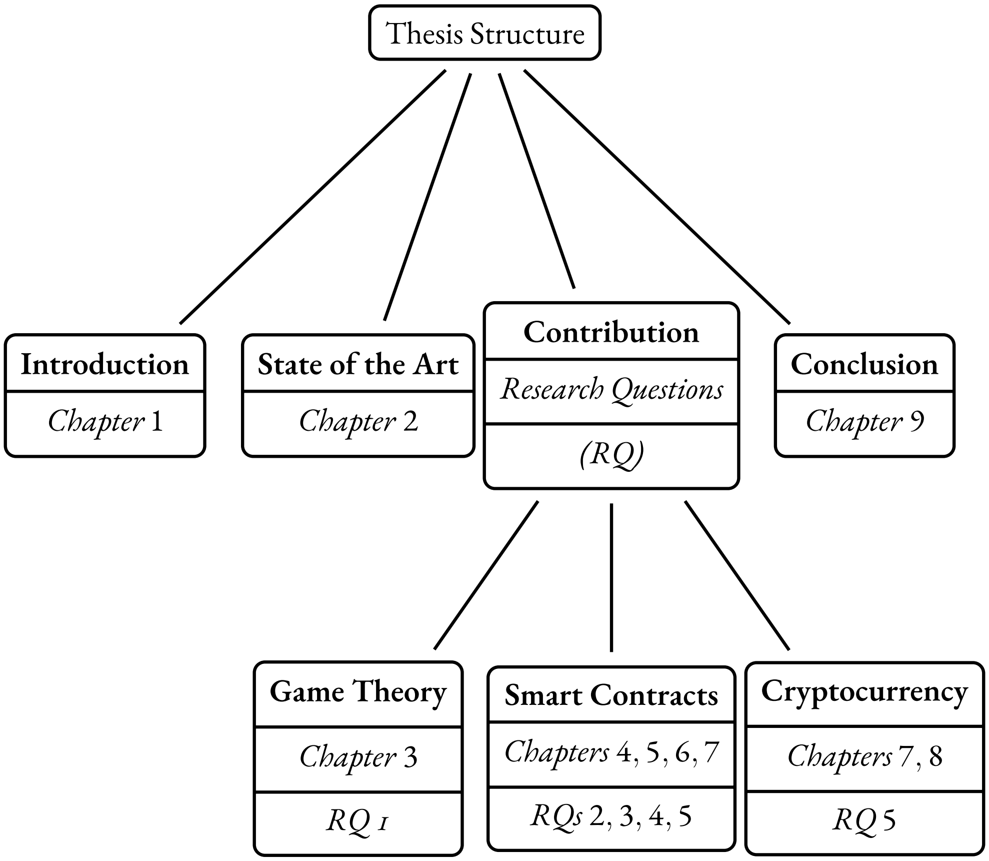


Figure 1.1: Graphical Layout of the Thesis based on the CS Concepts Employed

1. Khan, N., Kchouri, B., Yatoo, N. A., Kräussl, Z., Patel, A. and State, R. (2020). **Tokenization of Sukuk: Ethereum Case Study**. *In Global Finance Journal, Special Issue: Islamic Finance, 2020*. Elsevier [105].

2. Khan, N., Ahmad, T., Patel, A. and State, R. (in press). **Blockchain Governance: An Overview and Prediction of Optimal Strategies Using Nash Equilibrium**. *In the 3rd American University in the Emirates International Research Conference, AUEIRC 2020*. Springer [102].

3. Khan, N. and Nassar, M. (2019). **A Look into Privacy-Preserving Blockchains**. *In the Workshop on 16th ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2019*. IEEE [107].

4. Khan, N., Ahmad, T., State, R. (2019). **Feasibility of Stellar as a Blockchain-based Micropayment System**. *In 2nd International Conference on Smart Blockchain, SmartBlock 2019*. Springer [104].

5. Khan, N., Ahmad, T. and State, R. (2019). **Blockchain-based Micropayment Systems: Economic Impact**. *In ACM IDEAS '19 Proceedings of the 23rd International Database Engineering & Applications Symposium (2019)*. ACM [103].

6. Khan, N. and State, R. (2019) **Lightning Network: A Comparative Review of Transaction Fees and Data Analysis**. *In Blockchain and Applications - International Congress (2019)*. Springer [109].

7. Khan, N. and Ouaich, R. **Feasibility Analysis of Blockchain for Donation-based Crowdfunding of Ethical Projects**. (2019). *In Smart Technologies and Innovation for a Sustainable Future. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). (2019)*. Springer [108].

8. Khan, N. (2018). **FAST: A MapReduce Consensus for High Performance Blockchains**. *In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, BlockSys@SenSys 2018*. ACM [101].

9. Khan, N., Lahmadi, A., Francois, J. and State, R. (2018). **Towards a Management Plane for Smart Contracts: Ethereum Case Study**. *In NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium (2018).* IEEE [106].

10. Keogh, J. G., Rejeb, A., Khan, N., Dean, K. and Hand, K. J. (in press). **Data and Food Supply Chain. Blockchain and GS1 Standards in the Food Chain: A Review of the Possibilities and Challenges**. (2020). *In Building the Future of Food Safety Technology, 1st Edition, Blockchain and Beyond 2020*. Elsevier [97].

11. Keogh, John G., Dube, L., Rejeb, A., Hand, Karen J., Khan, N. and Dean, K. (2020). **The Future Food Chain: Digitization as an Enabler of Society 5.0**. *In Building the Future of Food Safety Technology, 1st Edition, Blockchain and Beyond 2020*. Elsevier [96].

12. Yakubov, A., Shbair, W., Khan, N., State, R., Medinger, C. and Hilger, J. (2020). **BlockPGP: A Blockchain-based Framework for PGP Key Servers**. *International Journal of Networking and Computing* [199].

13. Lacasse, R: M., Lambert, B. and Khan, N. (2018). **Islamic Banking - Towards a Blockchain Monitoring Process**. *In Journal of Business and Economics* [160].

As a part of this research we presented two papers in finance conferences, where the abstracts of the papers were published in the *Book of Abstracts* in the conference proceedings. The concerned papers are given below:

I Khan, N., Kchouri, B. and Patel, A. (2020). **Tokenization of Sukuk: Ethereum Case Study**. *In International Conference on the Contemporary Issues in Finance, Trade and Macroeconomy, ICOFINT 2020*.

II Lacasse, R. M., Lambert, B. and Khan, N. (2017). **Blockchain Technology - Arsenal for a Shariah-Compliant Financial Ecosystem**. *In* 5th *International Conference of Entrepreneurial Finance, CIFEMA 2017*.

The above papers were enhanced post presentation. Thereafter, paper I got published as [105] while paper II got published as [160].

A paper, which is a part of this dissertation, is under review:

i. Khan, N., Lahmadi, A., Kräussl, Z. and State, R. (under review). **Management Plane for Differential Privacy Preservation through Smart Contracts**. *In the* 17*th* *ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2020*.

1.3.1 References to Publications

Chapter 2 contains a reference to publication 8, [101]. Chapter 3 is inspired from publication 2, [102]. Chapter 4 uses content from publication 9, [106]. Unit I of Chapter 5 derives inspiration from publication 3, [107]. Chapter 6 uses content from publication 1. Chapter 7 has been inspired from the work in publication 7, [108]. Unit I of Chapter 8 deals with publication 5, [103] while Unit II of the same chapter includes work from publication 4, [104]. Unit III of Chapter 8 derives its content from publication 6, [109].

If I have seen further than others, it is by standing upon the shoulders of giants.

Isaac Newton

2

Background and State of the Art

Traditional databases with a central authority are no longer an attractive proposition for users, who want to have more control and transparency in their transactions. Blockchain provides a distributed database that transfers the control to the users instead of a central authority and the ability to transfer assets absolving the need for intermediaries. The chapter gives a review of blockchain, smart contracts, decentralized finance and micropayments.

2.1 Blockchain

Blockchain is categorized under distributed ledger technology and is characterized by a **peer-to-peer network** and a **decentralized distributed database** as depicted in Fig. 2.1. Nodes in a blockchain network can either be validator nodes (miners in Ethereum and Bitcoin), that participate in the consensus mechanism or non-validator nodes, referred to simply as nodes. When any node wants to add a transaction to the ledger, the concerned transaction is broadcasted to all the nodes in the peer-to-peer

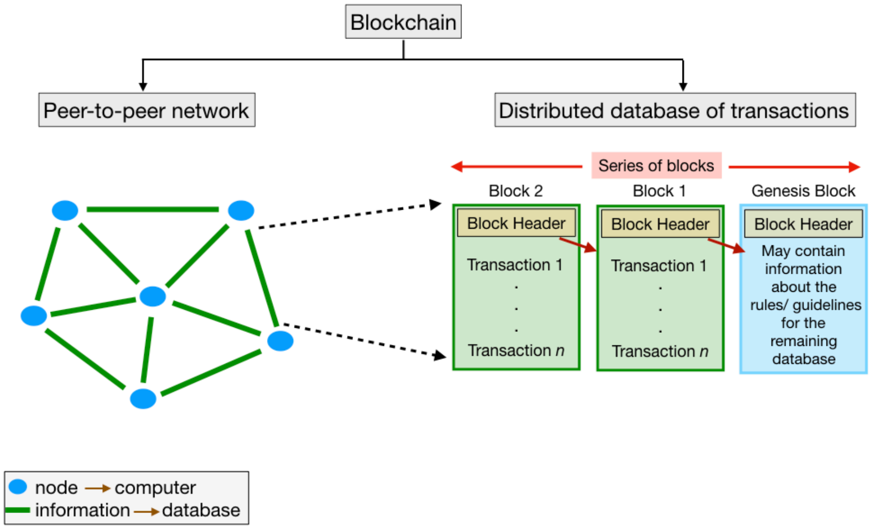


Figure 2.1: Diagrammatic Representation of Blockchain

network. The addition of transactions to the blockchain necessitates a consensus mechanism, which has been elaborated upon in 2.1.1. The validators compete with each other to see if their local block becomes the next block to be added in the blockchain. The consensus methodology employed by the underlying blockchain platform designates the validator, whose block gets added to the blockchain with the others remaining in queue and participating in the next round of consensus. The validator node gains an economic incentive for updating the blockchain database. Blockchain imposes restrictions on reading the data and the flexibility to become a validator depending upon whether the blockchain is permissioned or permissionless.

Blockchains can be categorized as public and private. Public blockchains like Bitcoin and Ethereum allow any user to read as well as update the database. In contrast to the public, is the private blockchain, which comprises of a group of validators with the probability of existence of a trust relationship between them and with cryptographic auditability provided by the chain of blocks. The major proponent of blockchain inception is that it *absolves the need to trust intermediaries or third parties* to enable online transactions while providing *auditable transparency*. Bitcoin was the first blockchain platform to be launched. Other blockchains like Ethereum, Hyperledger, Stellar and BigChainDB among others followed.

2.1.1 Consensus

A consensus algorithm enables secure updating of the blockchain data, which is governed by a set of rules specific to a blockchain platform. *Proof of work* [138], *Proof of Stake* [119] and *Byzantine Fault Tolerant* consensus protocols [28, 25, 129] are the major consensus algorithms being used. There are other consensus protocols too, like *Proof of Elapsed Time* [32] and *Proof of Authority* [51], to name a few. The different consensus protocols used are tolerant to different kinds of faults and a classification of faults [1] with the consensus protocols resilient to them is indicated in Table 2.1. The consensus protocols listed resilient to the faults is not an exhaustive list but is intended to give an indication on the commonly used ones. Temporal failures like message delays pose insignificant issues in a public blockchain like Ethereum but in a private blockchain, message delays can be used to launch a 51% attack [142].

Table 2.1: Fault Tolerance in Different Consensus Protocols

Fault	Description	Resilient consensus protocols
Crash failure	node ceases to function	PoW, PoS, SCP, BFT, PBFT (depends on the number of nodes failed)
Omission failure	node fails to give the expected output	most consensus protocols
Transient failure	node fails temporarily	most consensus protocols
Byzantine failure	node fails arbitrarily	PoW, PoS, BFT, PBFT, SCP, Tendermint
Temporal failure	message delays	PoW, PoS, SCP (used in a public blockchain)
Security failure	vulnerable to attacks e.g. Sybil	none

The right to update the blockchain data is distributed among the economic set [2]. An economic set is a group of users that can update the blockchain based on a set of rules. The economic set is intended to be decentralized with no collusion by a group within the set to form a majority even though they might have a large amount of capital and financial incentives. The blockchain platforms that have emerged employ one of the following decentralized economic sets, where each might utilize a different set of consensus algorithm.

[1] Karmakar, S. http://www.iitg.ac.in/psm/qip2015/material/Sushanta_Karmakar_Lectures.pdf. Accessed April 11, 2020.

[2] Buterin, V. (2014). Proof of stake: How I learn to love weak subjectivity. *Ethereum Blog*.

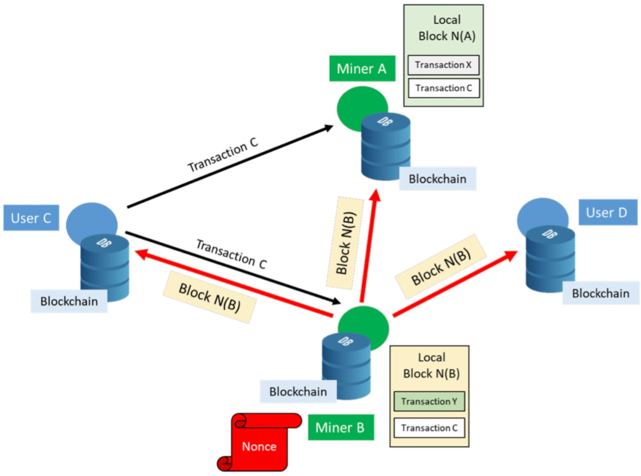


Figure 2.2: Mining in PoW Consensus Systems

Owners of Computing Power

This set employs Proof of Work (PoW) as a consensus algorithm observed in blockchain platforms like Bitcoin and Ethereum. Each block header in the blockchain has a string of random data called a nonce attached to them. The miners (validators) need to search for this random string such that when attached to the block, the hash of the block has a certain number of leading zeros and the miner who is able to find the nonce is designated to add his local block to the blockchain accompanied by the generation of new cryptocurrency. This process is termed as mining and is depicted in Fig. 2.2. Every transaction in the block also has a hash. All the hashes of the transactions in a block are also hashed, sometimes several times, to produce the merkle root. The block hash depends on the nonce and the merkle root. Hashes are one-way functions so there is no easy way to find the right nonce or somehow engineer a block to be correct. Mining involves expensive computations leading to a wastage of lot of computational power and electricity, undesirable from an ecological point of view and leading to a small exclusive set of users who are ready to do mining. This exclusivity however goes against the idea of having a decentralized set leading blockchain platforms to employ other means of arriving at a consensus.

Stakeholders

This set employs the different variants of Proof of Stake (PoS) consensus mechanism. PoS is a more just system than PoW as the computational resources required to accomplish such mining or validation can be done through any computer. PoS requires that the miner or the validator locks a certain amount of their coins in the currency of the blockchain platform, for verifying the block. This locked amount of coins is called a stake. Computational power is required to verify whether a validator owns a certain percentage of the coins in the available currency or not. There are several proposals for PoS. PoS enables a better decentralized set, takes the power out of the hands of a small exclusive groups of validators and distributes the work evenly across the blockchain. In Ethereum PoS, the probability of mining the block is proportional to the validator's stake just as in PoW it is proportional to the computational hashing power. As long as a validator is mining the stake owned by him remains locked. A downside of this kind of consensus is that the richest validators are accorded a higher priority though the mechanism encourages more community participation. Some consensus protocols use traditional Byzantine Fault Tolerance theory, BFT. However, in these kinds of protocols too, the economic set needs to be sampled for the total number of nodes. Mostly the set used is stakeholders and so such protocols can be considered as subcategories of PoS.

A User's Social Network

This is being used in Ripple [30] and Stellar [129] consensus protocols. The Ripple protocol for example requires a node to define a unique node list (UNL), which contains a list of other Ripple nodes that the defining node is confident would not work against it. A node consults other nodes in its UNL to achieve consensus. Consensus happens in multiple rounds with a node declaring a set of transactions in a 'candidate set', which is sent to other nodes in the UNL. Nodes in the UNL validate the transactions, vote on them and broadcasts the votes. The initiating node then refines the 'candidate set' based on the votes received to include the transactions getting the largest number of votes for the next round. This continues until a 'candidate set' receives 80% votes from all the nodes in the UNL and then it becomes a valid block in the Ripple blockchain.

2.1.2 Performance and Scalability

Blockchain came into inception with the launch of Bitcoin with the decentralized consensus proof of work. Bitcoin currently supports 7 transactions per second (henceforth referred to as 'tps'). If bitcoin were to come to the performance of Visa, 1667 tps [3] then it would lead to extreme centralization of the network with the miners having irrefutable power to charge high transaction fees [154]. A major limitation to achieving this throughput, ignoring the centralization, is the consensus mechanism. Proof of work consumes incredible amounts of energy comparable to Irish national energy consumption [4]. There is an economic incentive attached to update the blockchain, which motivates users to contribute to the consensus. The issue does not end at exploitative utilization of electrical power. Proof of work also involves computing power with the one in possession of high computing resources having a leading edge. 51% attacks to negate the immutable nature of blockchain can be launched with superior computing resources [120]. The consensus is thus, neither fair nor environmentally viable. The time to add a new block is given as 10 minutes in bitcoin and 15 seconds in Ethereum, though in reality the figures are way higher and network congestion increases this time.Thus, there is high latency between transaction submission and it's addition to the blockchain rendering the system misaligned as a payment system. In both the blockchain networks not all submitted transactions are added to the blockchain forcing resubmission on the part of the sender. The probability of transaction inclusion in Ethereum is given as 70% [5]. Scalability is also restricted as seen in Hyperledger where the network fails to function to scale beyond 16 servers [53]. Stellar too is working on integrating Lightning Network for a scalable blockchain platform.

In [68], Gervais et al. introduce a novel blockchain simulator to analyze the security and performance of proof of work blockchains like Ethereum. There is ongoing research on solving the scalabil-

[3] Vermeulen, J.(2016). VisaNet - handling 100,000 transactions per minute. https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html, accessed August 13, 2018.

[4] Jenkinson, G. (2017). Bitcoin mining uses more power than most African countries. https://cointelegraph.com/news/bitcoin-mining-uses-more-power-than-most-african-countries, accessed August 13, 2018.

[5] ETH Gas Station. (2017). Current dynamics of transaction inclusion on Ethereum. https://medium.com/@ethgasstation/current-dynamics-of-transaction-inclusion-on-ethereum-ae8912edc960, accessed August 7, 2018

ity and throughput issues related to blockchain platforms, while maintaining a decentralized infrastructure. In [53] a benchmarking framework has been proposed to analyze private blockchains focusing on the performance metrics of existing blockchain platforms. [69] negates the assumption that information dissemination in the Bitcoin blockchain network is directly received by the nodes. Zhao et al. [204] demonstrate how the average number of transactions and the average confirmation time of the transactions differs with the mining parameter. In [198] an architecture for a private blockchain is proposed with three strategies for improving the scalability of private blockchain platforms while [145] addresses the efficiency issues in blockchain by conducting a review on recent significant work.

Kokoris-Kogias et al. propose *Omniledger*, a novel distributed ledger that preserves security in a permissionless environment and optimizes performance by inter-shard transaction processing, ledger pruning and a novel low-latency validation of low-value transactions [114]. In [113], a novel Byzantine consensus protocol, Byzcoin, is proposed that utilizes scalable collective signing to enable a commit of Bitcoin transactions in seconds, thereby achieving a throughput higher than PayPal. Berger and Reiser [17] conduct an analytical study on the various optimization techniques utilized in previous work to scale Byzantine consensus for deployment in large environments. Croman et al. [44] analyze how circumstantial and fundamental bottlenecks limit the throughput and latency in Bitcoin. In [79], Hao et al., propose *BlockP2P*, a novel optimization design to enhance broadcast efficiency while preserving the security. Alharby and Moorsel in [7] propose *BlockSim*, a framework developed in Python, to build discrete-event dynamic system models for blockchains. Aldweesh et al. propose a benchmark approach in [6] to conduct an assessment of computational resources required per Ethereum opcode. In [191], Wang designs malicious behavioural patterns and tests the impact of malicious behaviour on the performance of Hyperledger Fabric.

Rouhani and Deters in [166] conduct a systematic review of security methods and tools, decentralized applications and performance improvement approaches for smart contracts. Eyal et al. propose a new scalable blockchain protocol, Bitcoin-NG (Next-Generation) in [61], which is Byzantine fault tolerant and shares the same trust model as Bitcoin. Karame in [100] analyzes the security provisions of Bitcoin and its underlying blockchain with the results applicable to altcoins, that have evolved from Bitcoin source code. Oliveira in [147] conduct a comprehensive comparison between Parity and Multichain, focusing on the analysis of transaction-validation time, transaction-mining time, transaction-seek time and block-seek time. Rouhani and Deters in [165] analyze Ethereum clients, Geth and Parity, on a private blockchain to provide a better understanding of different clients on Ethereum performance.

Data Structure

A blockchain is a linked list of blocks with each block having a pointer to the previous one in the chain of blocks. Conceptually the first block, *genesis* block, has a pointer which points to null. Contrary to a linked list, a blockchain does not permit any modification to the list of existing blocks as each pointer is basically a hash of the previous block and any modification to the data in the block would change the resulting hash and make it different from the hash stored in the next block, which again goes on to contribute to the hash of the block in which it is present and functions as the pointer to the next one in the chain. A parallel technology, *directed acyclic graph*, DAG, is also a distributed ledger where the transactions are organized as nodes in a graph with the transactions joined to each other by directed links. DAG is visualized as a technology to enhance the performance of the blockchain. Zhou et al. in [206] propose a novel double-DAG permissionless blockchain, *DLAttice*, which is able to reach consensus in 10 seconds as opposed to the theoretical 10 minutes in Bitcoin.

Consensus Mechanism

Miller et al. in [133] propose *HoneyBadgerBFT*, an asynchronous BFT protocol, that guarantees liveness without any timing assumptions and a throughput of tens of thousands of transactions per second. Feng et al. in [62] propose a pruneable sharding-based blockchain protocol, that utilizes a sharding technique and PBFT to enhance security and scalability. In [70], a new cryptocurrency *Algorand*, based on a new Byzantine Agreement protocol, is proposed, which achieves transaction confirmation in under a minute, has a throughput of 150x times that of Bitcoin and is scalable. In [90], an evaluation of the performance of Raft consensus algorithm in networks with non-negligible packet loss rate is conducted.

2.1.3 Financial Applications

The finance industry can utilise the benefits offered by blockchain for all those transactions, where the loss of confidentiality is not desired/ ignored for the transparency the technology offers together with the reduced infrastructure costs by elimination of the need for intermediaries. A few applications have been mentioned below:

1. Smart Contracts. Any kind of business logic relying on data can be coded by way of smart contracts. Securities that are based on payments and rights, which are executed according to predefined rules can be coded as a smart contract in capital markets. Experiments are ongoing on the issuance of smart bonds. A pertinent example is Ethereum smart contracts.

2. Supply Chain Finance. Supply chain management comprises of tracking the origin and movement of items which can suffer from counterfeiting and theft. The financially critical items like bills of lading or letters of credit can be tracked by a blockchain taking away the possibility of a group of users from corrupting the documents and end users would have more trust in what they receive paving the way for a smart supply chain finance (SCF) [85]. Examples of companies using this technology are *Skuchain* and *Wave*.

3. Digital Assets. The finance sector is using blockchain to create digital assets like stocks, bonds and land titles. Examples of companies using this technology are *NASDAQ* and *Chain*.

4. Payment Systems. Bitcoins are being used to send money to anyone across the world and merchants are accepting bitcoins as payments. Each bitcoin is related to a particular user secured by means of an encrypted electronic signature. The movement of a bitcoin from one user to another user is recorded in the distributed ledger and the exchange take place by changing of the bitcoin address of the sender to the bitcoin address of the receiver imitating the transfer of physical cash from one wallet to another person's wallet. Examples of blockchain-based payment systems are *BitPay* and *Abra*.

5. Digital Identity. The blockchain ID can be used to sign digital documents or sign in to websites. Banks can be set up for authentication of such blockchain ID's or they can partner with

blockchain companies working on the same for facilitating instantaneous cross-border transactions. An example of a company offering such services is *Keybase*. However privacy issues need to be tackled in this context [77].

6. Data-Driven Decision Making (DDDM). DDDM is an approach to business governance that can be backed by verifiable data. It is a way to gain competitive advantage and a study conducted by MIT [6] found that organisations using this approach had 4% higher productivity and 6% higher profits. Blockchain provides a very efficient way of creating this verifiable record of any data, file or business process on the blockchain. A few examples are a verifiable audit trail of insurance claims and archiving of communication to create a verifiable record of a company's online conversations. Examples of companies using blockchain to assist in creating this verifiable record are *Factom* and *Proof of Existence*.

2.2 Smart Contracts

Smart contracts are heralded as the most important application of blockchain. A smart contract is a computer program that formalizes relationships over computer networks through a combination of protocols with user interfaces [179]. They form the base of blockchain-based decentralized applications, which might function as products or services for mass usage. Smart contracts reside and are executed on the blockchain, where the correct execution is enforced by the consensus protocol. It relies on a programming language provided by the blockchain platform to encode its operations and the ways to handle user transactions. It can implement a wide range of applications including gaming, financial, notary or computation [14]. The distinguishing feature in comparison to paper-based agreements is that smart contracts are computer programs with the capability of unilaterally applying strict rules and consequences on the basis of fresh data inputs. Further, the blockchain assures that everyone is seeing the same thing without the reliance on having to trust each other.

Bitcoin, the first blockchain platform to be launched, does not support complex smart contracts.

[6] MIT study: Data-driven decisions mean higher productivity, profits, https://searchbusinessanalytics.techtarget.com/news/2240035852/MIT-study-Data-driven-decisions-mean-higher-productivity-profits

There is the availability of using simple smart contracts, but their execution is costly and designing is cumbersome [48]. Bitcoin uses a scripting system where every transaction is associated with a script, which upon execution acts as a precursor to the transaction execution. The programming language used is Script, which is stack based and not Turing complete restricting the usage of loops. A Bitcoin script contains instructions for the transaction that indicate to the receiver of funds, how the funds can be accessed for further utilization.

The main platform for implementing smart contracts is Ethereum and its high level programming language Solidity, which is Turing complete and compiled into bytecode language. Each compiled smart contract is stored in the blockchain and executed by the Ethereum virtual machine (EVM) running on the network nodes. Each operation in the EVM consumes gas. Gas is the metering unit for the use of Ethereum and helps in the calculation of fees in Ether per operation. A Solidity based smart contract is composed of a set of functions which are invoked by the contract users by sending transactions to the blockchain to validate their effects by the network. There are numerous other blockchain platforms that are providing the functionality of smart contracts. Ripple has invested in a smart contract platform, Flare[7], which is still being tested and was therefore not in consideration for our discussion. Stellar is not a typical blockchain supporting smart contracts as it does not have a smart contract programming language or a virtual machine to support the execution of smart contract code and is hence not a part of the review process. A comparison of the prominent platforms is given in Table 2.2

The work [128] provides a GUI-based tool for users to easily create more secure smart contracts. They also provide a set of design patterns as plugins for developers to enhance security and functionality of the smart contract. In [9] Anderson et al. categorize the Ethereum transactions into currency transfers and contract creations. In the work by Bartoletti et al. [14], the authors make a quantitative analysis of the usage and programming of a smart contract in Ethereum. In [181] Cook et al. develop DappGuard to monitor incoming transactions for any smart contract it manages with the intent to

[7] Ajiboye, T. (2020). Ripple backs new platform for smart contracts Flare networks via its Xpring. https://www.coinspeaker.com/ripple-smart-contracts-xpring/, accessed April 17, 2020.

[8] Transaction Execution Application Language

[9] Federated Byzantine Agreement

[10] delegated Byzantine Fault Tolerance

[11] Leased Proof of Stake

Table 2.2: Comparison of Smart Contracts

Blockchain platform	Turing complete	Programming language	Consensus algorithm	Execution environment	Wallet Model	Public
Algorand	✗	TEAL[8]	PoS	Stack	account	✓
Bitcoin	✗	Script	PoW	Stack	UTXO	✓
Ethereum	✓	Solidity	PoW	EVM	account	✓
Hyperledger	✗	Go	FBA [9]	Docker	account	✗
NEO	✓	Kotlin, C++, VB.Net, F#, Java	dBFT [10]	NeoVM	UTXO, account	✓
Tezos	✓	Michelson	PoS	Michelson	account	✓
Waves	✗	Ride	LPoS [11]	Docker	account	✓

detect any potential vulnerabilities. In [115] Ahmed et al. propose a decentralized smart contract system to preserve transactional privacy on the blockchain.

2.2.1 Applications in Finance

Any kind of business logic relying on data can be coded by way of smart contracts. The applications of this technology in finance are as follows:

- Capital Markets. Securities that are based on payments and rights, which are executed according to predefined rules can be coded as a smart contract in capital markets. Experiments are ongoing on the issuance of smart bonds [50].

- Escrow Account. Smart contracts can easily be set up as escrow accounts monitoring the exchange between two parties. Real estate projects or selling the shares of a company can use smart contract driven escrow account to facilitate the conditional transaction. An instance would be that the buyer would transfer funds to the contract account and after the ownership has been fully transferred, the contract would automatically release the funds to the seller [110].

- Inheritance Law. Inheritance can be coded as a smart contract. The triggering condition that sets the contract into execution would be the death of a person. This would increase fairness in distribution of wealth, resolve any potential disputes that could arise by means of transparency and reduce the time and effort needed for the process of determination of the wealth allocation to different parties followed by the transfer of money to the respected family member.

- Loans. Lending money is a core activity of any financial institution. Automating the lending process through the blockchain [83] can result in cost reductions [127]. Loans can be set up as smart contracts on a blockchain together with the collateral ownership information. In case the borrower misses a payment or a few designated payments, then the smart contract can revoke the digital keys that allow access to the collateral.

- Cryptocurrency Wallet Accounts. Wallets can be set up and controlled by smart contracts. These can include conditional clauses like daily withdrawal limits and restrictions like money that can be spent only on certain kinds of assets, in a certain geographical area or between two dates and likewise. The possibilities are endless and the savings would be huge considering the global reach of a blockchain platform. These can serve as an alternative to bank accounts for the unbanked and underbanked community [103].

- Proxy Lawyers. When considering routine financial transactions, lawyers are involved in repetitively processing mundane tasks and yet consumers have to spend a large amount on their fees to have them go through their wills or contracts. Theoretically smart contracts can do a greater portion of what the lawyers do and using them to support the legal system would reduce the costs associated with the process. The smart contracts could function as an intermediate layer between transacting and going to court [52].

- Insurance. The smart contracts would reduce the operating costs, increase the speed of execution and there would be greater efficiency in claims processing. The transparency and lack of textual ambiguity in coded smart contracts would prevent legal disputes. There would also be less insurance fraud on account of the contract being pre-programmed according to some specific conditions [67].

2.3 Decentralized Finance

Blockchain absolves the need for intermediaries in financial transactions and this can result in cost reductions for financial initiatives. The decentralized database, which conducts transactions in real time across borders, has spurred innovative use cases in the financial domain built upon distributed trust or a trustless economy. The technology envisages a trustless financial domain by virtue of its incorporation as there is no reliance on a single entity or organization. Rather, the trustless model is derived from game theoretic concepts of economic incentives where each validator in the blockchain network, works optimally, to ensure a secure and robust network devoid of fraudulent transactions. This trustless economy differs from the existing one built upon transaction cost economics (TCE), where the focus is on opportunism in the open market by virtue of pre-existing trusted relationships [36]. Financial products and services developed to function in the decentralized system can be viewed as coming under decentralized finance (DeFi).

Decentralized finance enables innovative models in finance, where seamless, low cost transactions across borders enables an increase in access to financial models that were restricted to a certain privileged group of users. A pertinent example of this is tokenization of bonds, that has created new avenues for generating capital for small and medium enterprises (SMEs), has the potential to create an open marketplace and enable asset tokenization backed by smart contracts. Researchers and academics are examining the tokenization of physical assets [173] whereas the industry has launched initiatives to provide the outreach of bonds to a wider consumer base through tokenization. In Luxembourg, the rights of a luxury building were tokenized on the Ethereum blockchain, which reduced the operational costs and gave the freedom to investors to decide the extent of their down payment [12]. Decentralized applications, dapps, can be developed on blockchain to provide decentralized financial services to the masses. Similarly decentralized exchanges have emerged, like Bancor, together with payment networks, like Libra, to cater to this new growing financial domain. Fig. 2.3 depicts the functional architecture for access of products and services in DeFi. DeFi is composed of financial services like decentralized

[12] Machuron, C.-L. (2019). First real estate transaction via blockchain in Luxembourg. *Silicon Luxembourg*. https://www.siliconluxembourg.lu/first-real-estate-transaction-via-blockchain-in-luxembourg/. Accessed December 15, 2019

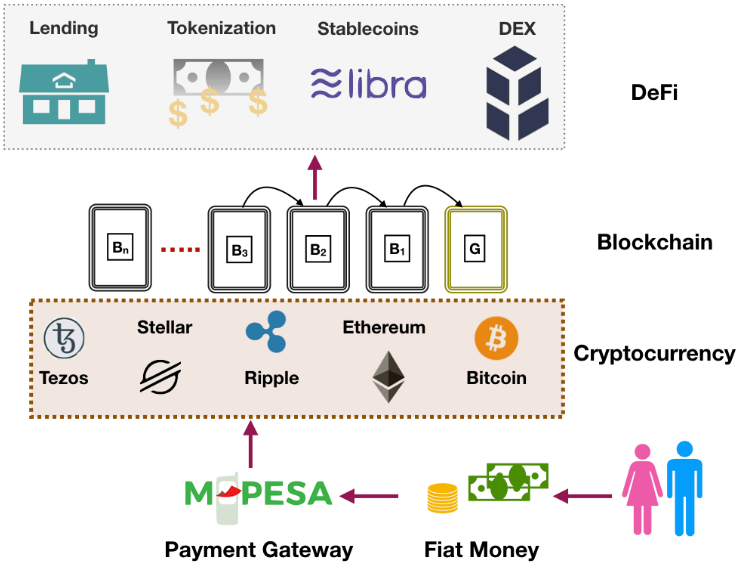


Figure 2.3: Functional Architecture of Access to DeFi

exhcanges (DEX), decentralized lending for home mortgages, tokenization of bonds and stablecoins like Libra from Facebook. At the user end, an exchange from fiat money to cryptocurrency is needed to be able to conduct transactions over the blockchain network for availing the products and services in DeFi. DeFi offers instant transactions recorded in the immutable, distributed blockchain database, where the execution is trusted to be enforced without fraud by the coupled strength of the validators in the blockchain network. Blockchain is represented by a series of blocks, namely *G* for genesis block followed by an ever-expanding chain of *n* blocks.

In chapter 6, we discuss the tokenization of investment certificates (sukuk) in the ethical finance domain achieved through a smart contract that was coded, deployed and tested on the local Ganache blockchain network as well as Remix-Ethereum IDE. Sukuk can be considered to be analogous to bonds in conventional finance. Listing 2.1 highlights the code for a function to distribute the profit accrued on the investment certificates (sukuk) on the basis of the payment frequency, which can be semi-annual or annual depending on the duration entered by the owner of the smart contract in the constructor passed during smart contract deployment. The functions needs the payment frequency to execute and can be called only by the owner of the smart contract. The investors are accessed through their Ethereum addresses and the profit distributed to the investor depends upon the number of sukuk (equivalent to bonds) owned by him and the profit rate, which was 4.75% in our use case. The number of sukuk coins owned by the investor increases on the basis of the profit accrued. The sukuk coins are tokens introduced to function only for the users registered through the smart contract to ensure security of fiat money held outside the blockchain and validity of ownership of the same. The exchange rate should be specified on the website of the issuer of sukuk.

```
pragma solidity 0.6.1;
function automaticPayment()public {
    require(now >= paymentFrequency);
    if(msg.sender!=owner){revert();}
    uint track;
    uint counter=numInvestors;
    while(counter>0){
        address i= investorList[track];
        uint factor=investors[i].ownSukuk;
        uint profit = (factor*475*proceedsPayment)/100;
        investors[i].profitReceived=profit;
        investors[i].sukukCoin+=profit;
        proceedsPayment-=profit;
        Transaction storage t=transactions[numTransactions++];
        t.sender=msg.sender;
        t.receiverID=investors[i].investorID;
        t.ID=numTransactions++;
        t.amount=investors[i].profitReceived;
        transactionList.push(t.ID);
        t.time=now;
        track++;
        counter--;
       }
}
```

Listing 2.1: Tokenization of Sukuk smart contract: function-Automatic Payment to Investors

We compare the issuance of sukuk without the blockchain as well as the issuance on both public and private Ethereum. We conduct a cost benefit analysis of the different scenarios, highlight the problems encountered during sukuk issuance without using the blockchain, elaborate on the circumvention achieved using Ethereum and conclude on the feasibility of tokenization of sukuk. Our undertaken study can be reviewed in the context of bonds as well and Table 2.3 compares the conventional issuance with a blockchain-based one, which we derived from our undertaken research in Chapter 6. A generalized review is given and more factual data can be accessed from Chapter 6 through the cost benefit analysis as well as the feasibility study of sukuk tokenization.

Table 2.3: Tokenization of Sukuk

Utility	Tokenization of sukuk	Conventional issuance
Number of Intermediaries	lower	higher
Denominations of issuance	much smaller	higher
Issuing body	startups, small and medium enterprises	large corporations, governments
Data	immutable	data integrity is questionable
Credit rating	use of AI on blockchain data for alternative credit scoring	lack of non-repudiated data
Standardization	customizable smart contract templates	lack of standardization, each sukuk issuance requires effort from scratch
Automation	automated periodic payments without incurring bank fees	involvement of bank
Cost incurred	comparatively lower	high

2.4 Micropayments

Financial technology implies deliverance of financial services with the aid of technology to consumers. The financial industry noted a marked increase in its outreach to the sections of society that were previously unbanked on account of lack of access to regulated financial institutions and poor economic status. Micropayments are a critical tool to enable financial inclusion and to aid in global poverty alleviation. The world presently has around 1.7 billion financially excluded adults. According to statistics provided by FINCA International, 76% of the poorest people, in 20 countries across Africa, Eurasia, Latin America, the Middle East and South Asia, are financially excluded [73]. Blockchain-based micropayment systems can provide the lower income group to have access to a means of payment for buying microproducts as well as to store, send and receive payments of small amounts in their community. It can prove to be an alternative for banking services for the lower strata of society.

Micropayments have been an active area of research and much effort has gone into analysis of the efficacy of micropayment systems, their need and technological innovations related to it. Pass and Shelat proposed a new lottery-based micropayment scheme for ledger-based transaction systems [151]. Burchert et al. proposed an addition of a third layer to Bitcoin to function as an enhancement for the second layer, Lightning Network, as a means to bring about cost reduction and scalability by trustless, off-chain channel funding [27]. Prihodko and Zhigulin proposed a new payment routing algorithm for Lightning Network [155]. Roos et al. proposed a decentralized routing for path-based transaction networks like Bitcoin and Ethereum [163].

Table 2.4 enlists a few micropayment systems and compares some of their characteristics:

1. **Medium of Exchange.** This defines whether the payment transfer is through a digital currency, fiat money or tokens.

2. **Scalability.** This concerns the throughput limit of the blockchain platform and is given in transactions per second (tps).

3. **Latency.** Micropayments should be conducted within a reasonable amount of time. The latency given in Table 2.4 for Lightning network and Raiden is for the use case where the payment channel needs to be opened and closed. Additionally in Raiden the token network contract needs to be deployed in Ethereum [109].

4. **Security.** Security is evaluated here on the basis of payment delivery in the midst of fraud. Both Lightning Network and Raiden have additional security provided by the underlying blockchain platforms of Bitcoin and Ethereum respectively.

5. **Privacy.** This deals with the availability of user data to third parties. Lightning Network and Raiden facilitate private transactions off the blockhain, whereas M-Pesa and PayPal provide

access to data to the third parties. Ripple and Stellar function like traditional financial institutions in terms of privacy where the user's data is under the security of the concerned financial institution.

6. **Prepaid or Postpaid.** This indicates whether users need to deposit cryptocurrency before or after a payment transfer.

7. **Interoperability.** This implies users of one system can transfer a payment to another system in another currency. Lightning Network is interoperable with other cryptocurrencies if they have the same hash function whereas Raiden permits atomic swaps with ERC20 tokens.

Table 2.4: Micropayment Systems

Features	Lightning Network	M-Pesa	PayPal	Raiden	Ripple	Stellar
Medium of exchange	BTC	Fiat, BTC	25 fiat currencies	ERC20 tokens	XRP	XLM
Scalability (tps)	billions	1200[13]	193 [14]	billions	65,000+[15]	1000[16]
Latency	1200+ sec	instant-24 hrs	few min -1 hr	42+ sec	5-7 sec	3-5 sec
Security	timelocks	SSL	SSL	smart contracts; hashlocks	Ed25519 keys	Ed25519 keys
Privacy	✓	✗	✗	✓	traditional	traditional
Prepaid Postpaid	✓ ✗	✓ ✓	✓ ✓	✓ ✗	✓ ✗	✓ ✗
Interoperability	✓ (crypto)	✓ (fiat, BTC)	✓ (fiat)	✓ (ERC20 tokens)	✓ (fiat, BTC)	✓ (fiat, crypto)

[13] https://www.the-star.co.ke/counties/2018-12-21-m-pesa-gears-up-for-1200-transactions-every-second/

[14] Steemit,https://steemit.com/cryptocurrency/@steemhoops99/transaction-speed-bitcoin-visa-iota-paypal

2.5 Conclusion

Blockchain platforms have a major limitation to achieving a throughput comparable to traditional payment networks with the causative agent being the consensus mechanism. PoW consumes incredible amounts of energy comparable to Irish national energy consumption [17]. In both Bitcoin and Ethereum, not all submitted transactions are added to the blockchain forcing resubmission on the part of the sender [108]. PoS suffers from 'nothing at stake' problem, where a designated user can update the blockchain state on every fork in the chain to have an economic gain despite the outcome of the fork. Byzantine agreement is seen in Hyperledger as Practical Byzantine Fault Tolerance, in Stellar as Federated Byzantine Agreement and in Tendermint coupled with proof of stake-based membership. Generally the membership in Byzantine Agreement systems is through a central authority. Decentralization is thereby reduced. Scalability is also restricted as seen in Hyperledger where the network fails to function to scale beyond 16 servers [53]. The implementation of Stellar involves the use of anchors analogous to PayPal, which brings in the need to trust intermediaries for payments. These bottlenecks motivated us to work on a new consensus mechanism, FAST [101], based on MapReduce [125] paradigm and Lamport's logical clocks [116], where research is in progress with promising preliminary results.

Smart contracts provided by blockchains offer a novel mechanism to enforce legal contracts through code. However, regulatory measures are still lacking in most of the countries and their legal status is questionable. Programming language used to write smart contract code, when Turing-complete, provides the advantage to write more complex contracts while introducing the probability of more errors, which post deployment on the blockchain can be exploited. Research is in progress for upgradable smart contracts as well as those that enable more private transactions [207].

DeFi is revolutionary for the finance industry with introductions of new models of financing ac-

[15] https://ripple.com/xrp/

[16] https://cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race

[17] Jenkinson, G. (2017). Bitcoin mining uses more power than most African countries. https://cointelegraph.com/news/bitcoin-mining-uses-more-power-than-most-african-countries, accessed August 13, 2018.

companied by a reduction of the control traditional financial institutions had over transactions. However, the new paradigm is is still in its infancy and is marked by an absence of regulatory measures, vulnerable blockchain security, volatility in cryptocurrencies, lack of mass awareness and complexity of usage. In this scenario, decentralized financial products and services foretell considerable work before mass adoption can happen.

The low cost micropayment model provided by blockchains can serve to reach the underbanked and these systems can even aid in poverty alleviation by facilitating donations of a few dollars, with the blockchain ensuring that the funds reach the intended recipients [108]. Ripple and Stellar come across as more competent micropayment systems in respect of the throughput and interoperability, with Ripple taking the lead. Criticism on their functioning comes in the form of privacy being similar to traditional financial institutions and existence of deviation from true decentralization. Blockchain has still not resolved the core issues of scalability, throughput, timeliness, security and privacy. In view of the aforementioned and to ensure prevention of cybercrime, coupled with the requirement of ease of integration with legacy systems, Ripple and Stellar come across as viable blockchain platforms for usage in applications where smart contracts are not needed. Amongst blockchain platforms supporting smart contracts, Ethereum, NEO and Tezos should be in consideration for deployment as all employ Turing complete smart contract languages.

Raise your quality standards as high as you can live with, avoid wasting your time on routine problems, and always try to work as closely as possible at the boundary of your abilities. Do this, because it is the only way of discovering how that boundary should be moved forward.

Edsger W. Dijkstra

3

Governance of Blockchain Networks

Blockchain governance is a subject of ongoing research and an interdisciplinary view of blockchain governance is vital to aid in further research for establishing a formal governance framework for this nascent technology. In this chapter, the position of blockchain governance within the hierarchy of Institutional governance is discussed. Blockchain governance is analyzed from the perspective of Information Technology governance using Nash equilibrium to predict the outcome of different governance decisions. A payoff matrix for blockchain governance is created and simulation of different strategy profiles is accomplished for computation of all Nash equilibria. We also create payoff matrices for different kinds of blockchain governance, which are used to propose novel mathematical formulae usable to predict the best governance strategy that minimizes the occurrence of a hard fork as well as predicts the behavior of the majority during protocol updates.

3.1 Introduction

Blockchain is a technological innovation that works on the concept of distributed networks requiring the coordinated efforts of multiple agents that comprise the network. The different agents, like users, founders of the blockchain network and others have different incentives that need to be aligned to ensure a uniform and consistent progress of the blockchain network. This necessitates the requirement of a governance strategy, which consolidates the goals of the stakeholders of the blockchain network to develop incentives and strategies for the other agents in the network for providing network consistency and availability. It is predicted that an absence of an apt governance mechanism can stall and result in a sub-optimized blockchain network [63], leading to frequent soft and hard forks in the network. A hard fork, though undesirable, is a relatively cost effective solution to disagreements, when compared to a split on a traditional structure like the government.

Blockchain governance is a subject of ongoing research and as of now no formal definition of blockchain governance exists. The author attempts to give a formal structure to blockchain governance consolidating its position within the hierarchy of Institutional governance. The chapter elaborates on the various agents involved in a blockchain platform and gives an overview of their position in the broader vision of blockchain governance. The chapter discusses the three dimensions of IT governance as they apply to blockchain governance. Nash equilibrium is a concept within game theory, which has multiple applications in blockchain [122]. Nash equilibrium is used to predict the outcome of different governance implementation strategies to find an optimal strategy that minimizes the occurrence of hard forks. The scenarios of no blockchain governance, off-chain and on-chain blockchain governance are discussed, to conclude on the best scenario that minimizes the occurrence of hard forks, the occurrence of which is unavoidable in many cases.

The chapter is a pioneer in giving a multidisciplinary view of blockchain governance and using game theory concepts to analyze different governance strategies. A multi-faceted view of blockchain governance is given in Section 3.3 while Section 3.4 gives the relevant background on Nash equilibrium. Application of Nash equilibrium and simulations of the developed blockchain governance strategic game are accomplished to conclude on optimal strategy profiles in subsection 3.5.1. Payoff matrices are constructed for off-chain and on-chain blockchain governance and mathematically analyzed to derive formulae that can help in prediction of hard forks based on the choice of governance decision during a protocol update in subsection 3.5.2. Data from Ethereum fork is analyzed to verify the developed formulae in Section 3.6. The conclusion of the undertaken study is given in Section 3.7.

3.2 Related Work

Davidson et al. view blockchain governance from the perspective of Institutional governance [49]. Beck et al. focus on a research framework agenda for blockchain governance, deriving rules from IT governance [16]. Chohan discuss the governance issues in decentralized autonomous organizations [38]. Atzori elaborates on the key points of blockchain governance from a political perspective, focusing on the distinguishing characteristics from State authority, citizenship and democracy [12]. Reijers et al. do a comparative analysis of blockchain governance, espoused by blockchain developers with the governance concepts discussed within social contract theories [158]. Barrera and Hurder view blockchain policy upgrade as a coordination game and develop a simple model of strategic chain choice [13]. Arrunada and Garicano discuss that new forms of soft governance need to be developed that allow the decentralized network to avoid bad equilibria [10]. In this chapter, we discuss the hierarchy of Institutional governance within which blockchain governance resides and analyze IT governance as it applies in a blockchain organization. The implementation categories of blockchain governance is highlighted and Nash equilibrium is used to construct payoff matrices to predict the best implementation strategy for blockchain governance.

3.3 Blockchain Governance: Hierarchical Position and Description

The coordination of various entities that comprise a blockchain network to ensure that the network functions without conflicts to accomplish the strategic goals of the network requires a **governance** mechanism. The main components that comprise the blockchain network can be summarized as follows:

1. Validators

2. Users

3. Consensus Protocol

4. Governance Mechanism

According to Vitalik Buterin, the founder of Ethereum, governance is needed for the base layer in blockchain design, which comprises of the blockchain itself. A second layer above the base layer consists of protocols, such as auctions, cryptocurrency payments and dapps, that are built on top of the underlying blockchain, as depicted in Fig. 3.1. It is envisaged that governance is required for the base layer, layer 1, to ensure a robust functioning of the protocols in layer 2 [1]. Governance is defined by Vlad Zamfir, the co-founder of Ethereum, as "*the process by which we attempt to establish (or maintain/ revoke) the legitimacy of decisions, decision-making processes, and the related governance norms/ expectations*" [2]. Things that can influence the decisions are termed as upstream, with the involved actors known as participants. Things that get influenced by the decisions are termed as downstream, with the involved actors known as stakeholders as depicted in Fig. 3.1.

A blockchain network is analogous to an organization like Google or Microsoft, with it's own set of users, employees (validators), protocols and a governance structure. Consider the email services, Gmail provided by Google and Outlook by Microsoft, where their purpose is the same but the governance mechanisms of the two corporations, Google and Microsoft, differ. Services provided by a blockchain network, like cryptocurrency payments or dapps, can be comparable to the services provided by a technology company. The blockchain network built by an organization, example Stellar, will put it in the category of a technology company. Presently there are numerous organizations like Bitcoin, Ethereum and Tezos amongst others, providing a blockchain-based infrastructure. The organizations differ in their consensus protocols, governance mechanisms, services and strategic goals. Thus, a universal governance mechanism cannot exist for blockchain in the wake of multiple service providers for the technology.

[1] Buterin, V. (2018). Layer 1 should be innovative in the short term but less in the long term. https:

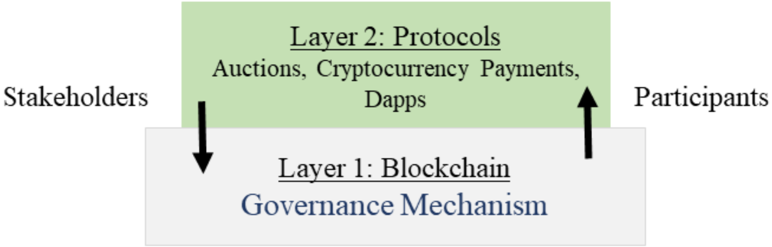


Figure 3.1: Blockchain Design

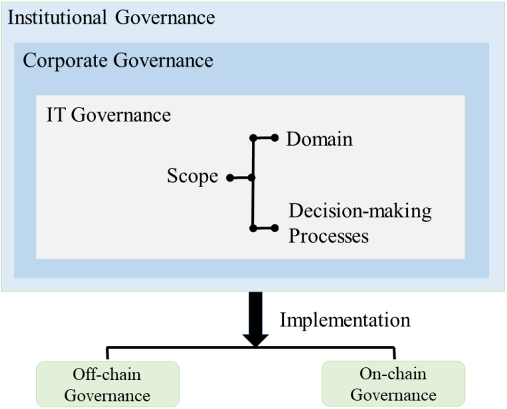


Figure 3.2: Hierarchy of Governance in Blockchain

The blockchain network facilitated by an organization will make the respective organizations be analogous to a technology company, where the standards and frameworks for corporate governance would be applicable. This view is corroborated by the domain of corporate governance, which indicates that "*Corporate governance includes all types of firms whether or not they are formed under civil or common law, owned by the government, institutions or individuals, privately or publicly traded*" [184]. This implies that firms like Stellar will be in the realm of corporate governance. Corporate governance is concerned with the relationship among the many players in an organization and the organizational goals for which governance is needed. The different players in an organization are the stakeholders, management, board of directors, employees, suppliers, customers, lenders, regulators, the environment and the community at large [71]. Corporate governance deals with the set of rules, processes and practices which aid in giving the organization a direction and a framework to ensure its functioning is within the defined parameters. Corporate governance lies within the realm of different Institutional governance systems [75]. Blockchain governance, ensuing from corporate governance would essentially follow the similar set of processes and rules to achieve the vision of the founders while ensuring that the participants in the network like the validators and users contribute to its goals. A good governance protocol would ensure that the blockchain would be environmentally-friendly, would minimize the occurrence of forks and changes in the code would represent the agreement of the majority of the agents in the blockchain network.

3.3.1 IT Governance

Information Technology (IT) governance is a critical driver for corporate governance. It is a component of corporate governance but the relationship between the two remains largely unexplored, despite the acknowledgement that an organization would fail to accomplish its goals without a good IT governance mechanism [39]. Weill and Ross describe IT governance as "*specifying the decision rights and accountability to encourage desirable behaviour in the use of IT*" [193]. This definition includes establishment of a set of processes and deciding the authorities for providing the input to making

`//vitalik.ca/general/2018/08/26/layer_1.html`, accessed September 7, 2019

[2] Zamfir, V. (2018). Ethereum Community Conference.

decisions. They indicate a set of questions that must be addressed for an effective IT governance mechanism, which includes the decisions that must be made for effective management and use of IT, delegation of authority for decision-making and finally the process of decision-making coupled with monitoring. Simonsson and Johnson pointed out that a shared definition is lacking in the field of IT governance [171]. They provided an IT governance definition based on consolidation of literature, which identified three dimensions namely, the domain, processes and scope in which IT decisions are made and carried out. This work proceeds with the three dimensions that encompass IT governance stated in [171] and justifies the usage by ensuring conformity to the questions addressed by Weill and Ross in [193]. This work concentrates on IT governance as blockchain organizations are primarily technology initiatives increasing the significance of IT governance in the context of blockchain platforms.

Domain

The Domain dimension includes the entities, the decisions should consider and comprise of goals, processes, people and technology [171]. In the context of blockchain technology, goals of any public blockchain technology majorly encompass the characteristics of a blockchain platform, which are as follows:

1. Trustless: The technology does not depend on intermediaries and third parties for conducting transactions.
2. Immutable: The ledger is incorruptible, being verified by innumerable nodes and cryptography ensures a permanent record of transactions.
3. Decentralization: The technology is not controlled by a single entity and power is distributed.
4. Availability: The technology does not have a single point of failure.
5. Auditability: The immutable blockchain ledger is verifiable by anybody.
6. Confidentiality: The technology is public yet the identities of the users remain pseudonymous.

The goals outlined above might differ in some parameters in case of consortium and private blockchain networks. Additional goals of development of advanced protocols for enhancement of performance, monitoring of protocol updates or changes and alignment to the goals of the stakeholders also exist.

Examples of processes in blockchain include the implementation and management of peer to peer network, the distributed ledger, cryptographic algorithms involved, code development and prompt error corrections on detection. The people involved are the core developers that create the code to manage the functioning of blockchain technology, full nodes that maintain a copy of the entire blockchain ledger to put the code into action, the organisation, which manages the funds and reimburses the core developers and the users, who use the blockchain network. The organization can be for profit like Ripple, or non-profit like Stellar. Technology broadly includes the hardware required and the software that aids in the setup and implementation of the blockchain network.

Decision-making Process

The second dimension of IT governance is the decision-making process [171]. Decision-making process involves three phases where the matter under consideration is thought over, deliberated and then transformed into a model. The model is investigated and then implemented in the organization, which is monitored for performance evaluation. In the context of blockchain governance, the first phase in which the subject in focus is consolidated with facts can be considered equivalent to the protocol submission in Ethereum as EIP (off-chain governance (see 3.3.2)) or proposal submission in Tezos (on-chain governance (see 3.3.2)). The protocol can then be implemented in the testnet as in Tezos and voting ensues to deliberate upon its acceptance. If a majority is reached in the voting process involving the decision-makers, the protocol is implemented in the main blockchain network and monitored for any software bugs. Thus, the process is similar to IT governance and a formal framework would necessitate the adherence to all the three phases in order.

Scope

The last and third dimension in the definition of IT governance involves a discussion on the scope. Every governance decision implies a long and a short term aspect with a correlation between the time-line of the decision and the level at which it is made [171]. The scope dimension encompasses tactic and strategic decisions. In the context of a blockchain network, tactic governance decisions can be changing the user interface of the blockchain network whereas a strategic decision would involve a protocol update.

A brief discussion of the three dimensions of an IT governance framework as it applies to designing an effective blockchain governance mechanism indicates that the questions that need to be addressed for an effective governance framework as per Weill and Ross [193] have been majorly targeted. However, as per the definition of IT governance "*to encourage desirable behaviour in the use of IT*", there is a clear indicator on the use of incentives, which can be both monetary and non-monetary. The emphasis on incentives is less in this definition but they have been recognized as pivotal in the design and evaluation of any information system [177]. When the blockchain network is designed such that the users are encouraged and incentivized to use the network as per the design objectives then a very important design goal is accomplished. This incentive alignment can be derived from the theory of Nash equilibrium [86] or the principles of game theory as they apply to institutional economics [196]. Fig. 3.2 represents the hierarchy of governance in blockchain.

3.3.2 Implementation Methodologies for Blockchain Governance

The implementation of blockchain governance can be either off-chain or on-chain. Off-chain governance is seen in Bitcoin and Ethereum, which is characterized by an informal decision-making process independent of the underlying blockchain code base. Off-chain governance resembles the traditional governance mechanisms with relative centralization and distribution of power between the blockchain agents. Users who lack the technical expertise or the requisite financial resources fail to contribute to the governing decisions. The off-chain design mechanism for governance is driven by the belief that governance is an unpredictable and emergent phenomenon, which cannot be hard-coded into the blockchain in advance. The protocol updates are submitted by the core developers in the form of formal improvement proposals, for example as Bitcoin Improvement Proposals (BIPs) in

Bitcoin [3]. The e-proposals are then deliberated through social media and discussion groups. One of the issues with off-chain governance is lack of incentives for the proposers, which can lead to a small group of developers submitting proposals and hence centralization.

On-chain governance embodies the spirit of decentralization in the governance mechanisms as seen in Tezos. The concentration of power witnessed in off-chain governance strategy is minimized and the governance is implemented by virtue of a series of processes as opposed to a simple majority consensus. The exact procedure in on-chain governance might vary between different blockchain platforms. The proposals are submitted on-chain, voted and if agreed upon are deployed on the blockchain testnet for a designated amount of time. If the final vote is in favor after the testnet deployment, then the proposal is incorporated in the main blockchain. In order to achieve the settlement, governance rules are written into code and are a part of the blockchain enhancing transparency. It also reduces the turnaround time for a proposed protocol update. The infrastructure required for a well-functioning on-chain governance is huge comparatively and research is in progress for the requisite coordination tools that facilitate an efficient communication in on-chain governance [4].

3.4 Nash Equilibrium

Non-cooperative games in game theory are those where competition exists amongst the individual players and it is characterized by an absence of rules that enforce cooperative behaviour. Blockchain platforms can be viewed as non-cooperative games between the validators, who compete to add the next block to gain an economic advantage. Nash equilibrium can be used to derive a solution for non-cooperative games and can be utilized to aid in predicting optimum equilibria in blockchain governance [13]. In the mathematical context, if it is proved that a Nash equilibrium exists then this is equivalent to proving that a solution exists for a fixed-term problem [118]. Nash equilibrium introduced the concept of games with n participants, *players*, where each would need to decide on a course

[3] districtOx Education Portal. (2019). Off-Chain governance. https://education.district0x.io/general-topics/what-is-governance/off-chain-governance/, accessed September 1, 2019.

[4] Perez, Y. B. (2019). The controversies of blockchain governance and rough consensus. https://thenextweb.com/hardfork/2019/01/25/the-controversies-of-blockchain-governance-and-rough-consensus/, accessed September 15, 2019.

of action, *strategy*. Strategies can be *pure* or *mixed*. A pure strategy gives the moves a player will make during the course of the game under any situation. In blockchain governance, it represents the set of all possible choices a player can make. Mixed strategies are probability distributions over decisions as in the context of choosing a proposal, different agents in the blockchain network will choose one from the available choices ensuring that all the choices are taken by a random proportion of the agents. A pure strategy is analogous to a degenerate case of a mixed strategy, where the concerned pure strategy is chosen with a probability 1, whereas all others are chosen with a probability of 0.

Nash Equilibrium

It can be stated as a "*set of strategies, one for each of the n players of a game, that has the property that each player's choice is his best response to the choices of the n-1 other players*" [86] [140]. A payoff matrix is used to represent the available strategies and the players, where each cell of the matrix gives the outcome of different choices by each player. The matrix gives the outcome of an individual's choice of strategy in terms of gain or loss that a player undergoes, when his choice of strategy is executed, given the choice of other players. Thereafter, the matrix is analyzed to determine optimal strategies. John Nash in [140] defined that a *n-person game* is a set of *n players* or *positions*, where each player, *i*, has a finite set of pure strategies and a payoff function, p_i, mapping the entire set of *n-tuples* of pure strategies into real numbers. The term *n-tuples* implies a set of *n* items, where each item is associated with a different player [140]. The mixed strategy of a player is a collection of positive numbers that are in one to one correspondence with his pure strategies and have unit sum. The payoff function p_i is characterized by a unique extension to the *n*-tuples of mixed strategies and is linear in the mixed strategy of each player. The equilibrium point is a *n*-tuple where each player's mixed strategy maximizes his payoff if the strategies of other players is not changed. Thus, at equilibrium point each player's strategy is optimal against those of others [140].

Pareto Optimality

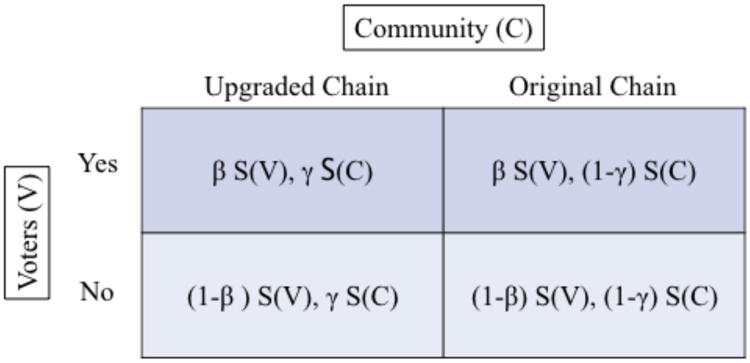
In game theory if a solution is Pareto optimal, then this implies that the strategy profile is such that there can be no other strategy in which a player's payoff can be increased, without decreasing the payoff of at least one other player. A strong Nash equilibrium, which implies stability against unilateral deviations of players and also against unilateral deviations of any subcoalition of players, is Pareto optimal [23].

3.5 Application of Nash Equilibrium to Blockchain Governance

Blockchain governance has some distinctive features differentiating it from traditional corporate governance processes:

- Decentralized nature of governance where the main role of the governance mechanism is to steer the community to achieve certain outcomes without having explicit levers to achieve these outcomes.
- Possibility of forks or opting out if the outcome is not aligned with individual goals is relatively hard wired in the whole governance process unlike the corporate setting where the cost benefit of opting out are quite high and in many cases might imply starting completely afresh.
- The decision of the individual on a blockchain platform is based not just on an individual choice but the impact that it is likely to have on the entire blockchain network, through the communities collective decision, resulting in a network effect.

We have applied Nash equilibrium to blockchain governance and simplified the governance process as a two player strategy game, where voters **(V)** are a group of **k** entities involved in the voting of acceptance and rejection of a proposal, which is the decision-making process when viewed from the perspective of IT governance. The impact of the decision will be on the broader community **(C)** connected to the blockchain and comprising of **n** entities. The payoff matrix for our evaluation is given in Fig. 3.3. β represents the proportion of voters, **V**, who voted to accept the proposal by a **Yes** whereas γ represents the proportion of the broader community moving to the upgraded chain once a proposal is accepted based on the outcome of the voting process. **V** comprises of validators, who validate the transactions in blockchain, developers, blockchain token holders, blockchain stakeholders and any user of the blockchain platform who participate in the voting process of any new blockchain



		Community (C)	
		Upgraded Chain	Original Chain
Voters (V)	Yes	β S(V), γ S(C)	β S(V), (1-γ) S(C)
	No	(1-β) S(V), γ S(C)	(1-β) S(V), (1-γ) S(C)

Figure 3.3: Payoff Matrix for Blockchain Governance Game

proposal under consideration. **C** consists of all blockchain users who will be affected by the decision, including **V**. Whenever any proposal to update the blockchain code is initiated, the individual members of **V** must decide if they want to vote to accept the proposal, **(Yes)**, or reject the same **(No)**. Once the voting cycle for a new proposal is over, and there is no uniform consensus, the individual (in larger C) must choose between two chains: stay on the original chain **(O)** or join the new upgraded chain with an updated policy **(U)**. The payoff matrix given in Fig. 3.3 enumerates two strategies, *Yes* and *No* for **V** as described formerly and **C** also has two strategies, which are *Upgraded Chain* and *Original Chain*.

$$V(k) = \{Y, N\} \subseteq C(n) = \{O, U\} \tag{3.1}$$

Payoff (S) is the cumulative of individual payoffs as a result of the decision. We have assumed no distinction between entities in the Voter, (V) and Community, (C) in the value of payoffs (S_v, S_c):-

$$S(V) = \sum_{i=1}^{k} S(V_i) = kS_v \tag{3.2}$$

$$S(C) = \sum_{i=1}^{n} S(C_i) = nS_c \tag{3.3}$$

3.5.1 Simulation of Blockchain Governance Game

We use the software tools for game theory, version 15.1.1, provided by the Gambit project [159] to simulate a 2 player strategy game for **V** and **C**, the payoff matrix of which is given in Fig. 3.3. Gambit was used to compute all possible Nash equilibria for different values of β and γ and the computation results are depicted in Table 3.1. Player 1 is **V** and player 2 is **C** in Table 3.1. An analysis of the computations in Table 3.1 is given below:

Table 3.1: Simulation of Blockchain Governance Game

Simulation #	β, γ	Nash Equilibria #	1: Yes	1: No	2: Upgraded Chain	2: Original Chain	V Payoff	C Payoff
1	1, 1	1	1	0	1	0	1	1
2	0, 0	1	0	1	0	1	1	1
3	1, 0	1	1	0	0	1	1	1
4	0, 1	1	0	1	1	0	1	1
5	1/2, 1/2	1	1	0	1	0	1/2	1/2
		2	1	0	0	1		
		3	0	1	1	0		
		4	0	1	0	1		
6	3/5, 7/10	1	1	0	1	0	3/5	7/10
7	1/5, 2/5	1	0	1	0	1	4/5	3/5
8	7/10, 1/5	1	1	0	0	1	7/10	4/5
9	7/20, 18/25	1	0	1	1	0	13/20	18/25

- **Simulation 1.** There is only one Nash equilibria, where 100% of V vote 'Yes' to accept the proposal and the entire broader community C moves to the upgraded chain.

- **Simulation 2.** There is only one Nash equilibria where 100% of V vote 'No' to reject the proposal and the entire broader community C stays on the original chain.

- **Simulation 3.** There is only one Nash equilibria where 100% of V vote 'Yes' to accept the proposal but entire C stays on the original chain, ignoring the outcome of the voting process.

- **Simulation 4.** There is only one Nash equilibria where 100% of V vote 'No' to reject the proposal but entire C still move to the upgraded chain, ignoring the outcome of the voting process.

- **Simulation 5.** There are 4 Nash equilibria. Equilibria 1 and 2 indicate that when 50% of V vote as 'Yes' to accept the proposal there are two optimal decisions for C, where C can either stay on the original chain or move to the upgraded chain. Equilibria 3 and 4 indicate that when 50% of the voters vote 'No' to reject the proposal, the optimal decision for C will again be that the community stays on the original chain or moves to the upgraded chain. In the equilibria for this simulation, the community will be divided.

- **Simulation 6.** In this the value of $[\beta, \gamma > 0.5]$. There is only one equilibria where 60% of V vote 'Yes' to accept the proposal and 70% of C move to the upgraded chain.

- **Simulation 7.** The value of $[\beta, \gamma < 0.5]$ and there is only one Nash equilibria. When 80% of V vote 'No' to reject the proposal, 60% of C stay on the original chain.

- **Simulation 8.** The value of $\beta > 0.5$ and $\gamma < 0.5$. There is only one Nash equilibria where despite 70% of V voting 'Yes' to accept the proposal, 80% of C stay on the original chain, ignoring the outcome of the voting process.

- **Simulation 9.** The value of $\beta < 0.5$ and $\gamma > 0.5$. There is only one Nash equilibria where 35% of V vote 'Yes' to accept the proposal, 65% of V vote 'No' and 72% of C move to the upgraded chain, ignoring the outcome of the voting process.

The above analyses can be concluded with the following observations:

1. The broader community, C can take a decision independent of the outcome of the voting process.

2. If the proportion of V voting 'Yes' or 'No' to a proposal is known, the payoff matrix in Fig. 3.3 can be used to predict the optimal outcomes for C.

3. When C is divided on the outcome as in simulation 5, then there will always be more members on either the original or the upgraded chain increasing the payoff of that chain.

3.5.2 Evaluation of Different Kinds of Governance

We evaluate three possible scenarios of blockchain governance. We analyze the case of no governance and then investigate the performance of off-chain and on-chain governance mechanisms on the payoff to the community under specific conditions. We derive mathematical formulae based on our evaluation to aid in the prediction of optimal strategies for blockchain governance and make the following assumptions for our analysis:

1. β is the proportion of the voters **V**, voting **Yes** to accept a new proposal and can be extended to represent the entire community **C**.

2. The proposal is accepted if the majority of voters vote **Yes** in favor of the proposal. This implies that $0.5 < \beta \leq 1$.

3. If $\beta = 0.5$, then the above majority rule, **2** will apply.

4. The broader community **C** moves to the upgraded chain, **U**, if the voting was in majority for the proposal acceptance as indicated by **2** and **3**.

5. **C** moving to the upgraded chain, **U**, indicates that $0.5 \leq \gamma \leq 1$.

6. Only two possibilities exist for the entire community, which is that they either stay on the original chain, **O** or move to the upgraded chain, **U** post the decision following the voting process. We have ignored that a section of the community can create a new hard fork, separate from the original and upgraded chain.

No Governance

In the scenario of no governance as depicted in Fig. 3.4 each **C** member is choosing the best possible option for their own benefit whenever any change is made to the chain. The individual decision-making

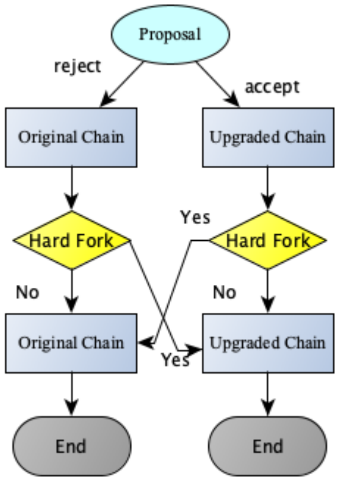


Figure 3.4: No Blockchain Governance

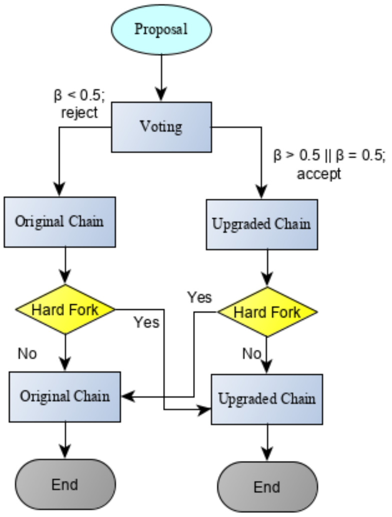


Figure 3.5: Off-chain Blockchain Governance

is complicated by a high degree of opacity in information exchange on proposed changes, relative payoff to the community and the possibility of hard fork occurring as a result of the change. Let γ be the proportion of **C** which chooses to move to the upgraded chain while $(1-\gamma)$ choose to remain on the original chain. The payoffs are reduced on both chains as compared to single-chain equilibria by a factor $[\gamma, (1-\gamma)]$ on **U**, **O** chains respectively. In equation 3.4, S_U represents total payoff in upgraded chain and in equation 3.5, S_O represents total payoff in original chain.

$$S_U = \gamma n S_C \leq n S_C \tag{3.4}$$

$$S_O = (1-\gamma) n S_C \leq n S_C \tag{3.5}$$

Off-chain Governance

Fig. 3.5 depicts the off-chain governance mechanism (see 3.3.2) with proportion β of voter community voting *yes* if there is no outright consensus. Depending on the majority preference, the chain is upgraded or the original is maintained. After the outcome is known, everyone has an option of stay-

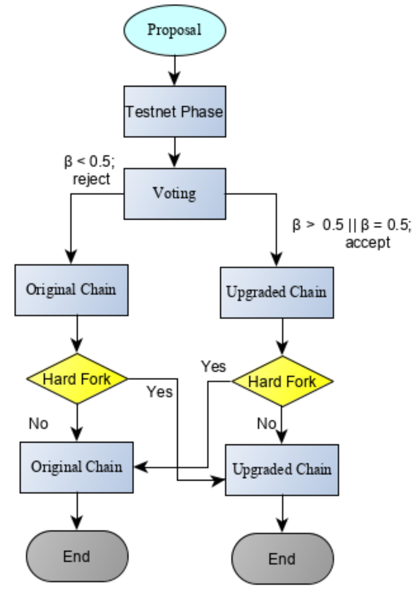


Figure 3.6: On-chain Blockchain Governance

ing on the upgraded chain or the original chain. The voting process is a group exercise while the hard fork decisions are individual. In this case with the information available, the member is more likely to go with the majority decision in order to maximize payoff, hence the probability of hard fork is lower than the previous case of no governance.

On-chain Governance

Fig. 3.6 depicts the on-chain governance mechanism (see 3.3.2), where the proposal is deployed on the testnet for voter community to use for a certain time period. The mechanism defers from the simple majority voting as in this case the objective is payoff maximization through maximum consensus. Thus a vocal minority which feels strongly about any proposed change has the possibility to convince the community during the testnet phase. If there is no uniform consensus after testnet phase, the proposals are put to vote with majority chain being chosen. The possibility of hard fork will remain but with an additional exchange round the probability of **C** group member going against the majority consensus reduces as compared to both the previous cases of no governance and off-chain governance.

3.5.3 Off-chain Governance: Payoff Matrices

We construct payoff matrices for off-chain blockchain governance using the basic blockchain governance matrix given in Fig. 3.3. We constructed 3 matrices of dimensions 2x2 for the respective values of β, γ indicated in the different rows of Fig. 3.7. We selected rows from the constructed matrices, which corresponded to the assumptions listed in subsection 3.5.2 and depicted them in a new matrix in Fig. 3.7. The matrix can be explained with the following strategy for **V**,**C**:

- If **V** validates the proposal as accepted then the chain is upgraded, the payoff is maximized and there is no threat of hard fork as shown in the cell, **A1** of the evaluation matrix. This is a pure strategy equilibrium. Equation 3.6 gives the surplus payoff for the voters S(V), while equation 3.7 gives the surplus payoff for the community S(C).

$$S(V) = S_{\text{Yes}} - S_{\text{No}} = kS_V \tag{3.6}$$

$$S(C) = S_U - S_O = nS_C \tag{3.7}$$

- If **V** does not validate the proposal but after a round of voting, majority chooses to go with the proposal there is risk of hard fork with members of **C**, who may feel the decision as tyranny of majority choosing to remain on the original chain. However surplus maximization still exists with upgraded chain, as depicted in cell **B1** of the payoff matrix, as $[0.5 < \beta, \gamma < 1]$. This is also Pareto optimal as compared to the original chain, **B2**, as members moving to alternate chain to increase their payoff always results in decreasing the payoff for others. Equation 3.8 gives the surplus payoff for the voters S(V), equation 3.9 gives the surplus payoff for the community and equation 3.10 gives the total surplus payoff S. When we compare the mixed strategy equilibria for cells **B1** and **B2**, we observe that the payoff in **B1** is more than in **B2**.

$$S(V) = S_{\text{Yes}} - S_{\text{No}} = \beta kS_V - (1-\beta)kS_V = (2\beta - 1)kS_V > 0 \tag{3.8}$$

$$S(C) = S_U - S_O = \gamma n S_C - (1-\gamma)nS_C = (2\gamma - 1)nS_C > 0 \tag{3.9}$$

$$S = (2\beta - 1)kS_V + (2\gamma - 1)nS_C > 0 \tag{3.10}$$

- If **V** does not validate the proposal but after a round of voting, majority chooses to stay on the original proposal there is again a risk of hard fork with some members of **C** choosing to go on the updated chain. In this case surplus maximization will be with original chain, **C2** as $[0.5 < 1-\beta, 1-\gamma < 1]$. This is also Pareto optimal as compared to the original chain, as seen in **C1** members moving to alternate chain to increase their payoff always results in decreasing the payoff for others. Equation 3.11 gives the surplus payoff for the voters S(V), equation 3.12 gives the surplus payoff for the community S(C) and equation 3.13 gives the total surplus payoff. Similar to the argument in the comparison of the payoff in **B1** and **B2**, the mixed strategy equilibria in **C2** when compared with the mixed strategy equilibria in **C1** has a higher payoff.

$$S(V) = S_{\text{No}} - S_{\text{Yes}} = (1-\beta)kS_V - \beta kS_V = (1-2\beta)kS_V > 0 \tag{3.11}$$

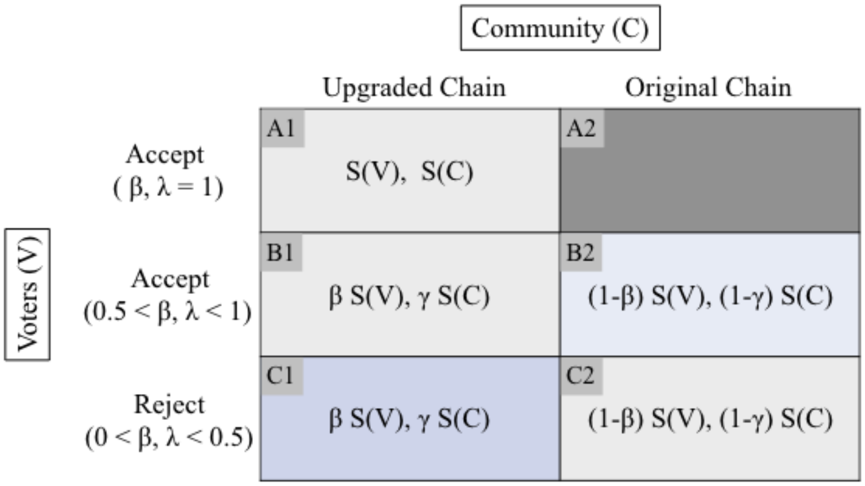
$$S(C) = S_O - S_U = (1-\gamma)nS_C - \gamma nS_C = (1-2\gamma)nS_C > 0 \tag{3.12}$$

$$S = (1-2\gamma)nS_C + (1-2\beta)kS_V > 0 \tag{3.13}$$

3.5.4 On-chain Governance: Payoff Matrices

We construct payoff matrices for on-chain blockchain governance using the basic blockchain governance matrix given in Fig. 3.3. We constructed 3 matrices of dimensions 2x2 for the respective values of β, γ indicated in the different rows of Fig. 3.8. We selected rows from the constructed matrices, which corresponded to the assumptions listed in subsection 3.5.2 and depicted them in a new matrix in Fig. 3.8. The matrix can be explained with the following strategy for **V**,**C**:

- If **V** validates the proposal as accepted then the chain is upgraded, the payoff is maximized and



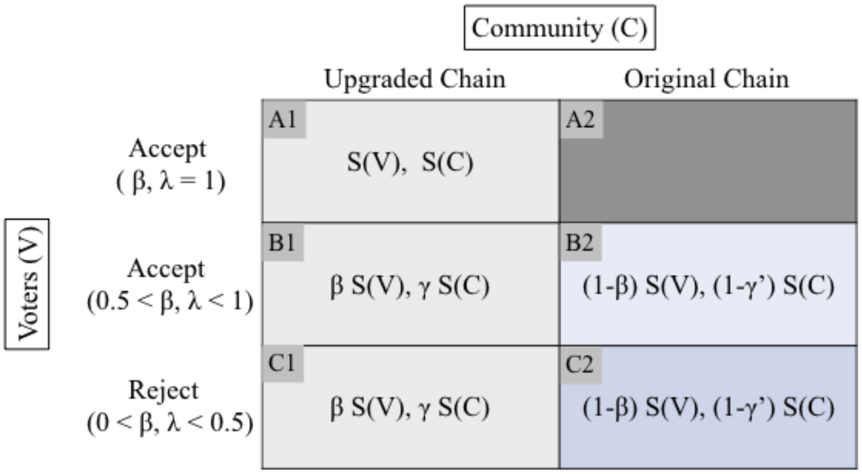
		Community (C)	
		Upgraded Chain	Original Chain
Voters (V)	Accept (β, λ = 1)	A1 S(V), S(C)	A2
	Accept (0.5 < β, λ < 1)	B1 β S(V), γ S(C)	B2 (1-β) S(V), (1-γ) S(C)
	Reject (0 < β, λ < 0.5)	C1 β S(V), γ S(C)	C2 (1-β) S(V), (1-γ) S(C)

Figure 3.7: Payoff Matrix for Off-chain Governance

there is no threat of hard fork as depicted in the cell, **A1** of the payoff matrix. This is a pure strategy equilibrium. Equation 3.6 gives the surplus payoff for the voters S(V), while equation 3.7 gives the surplus payoff for the community.

- If **V** does not validate the proposal and even after the testnet round there is no consensus, then the voting takes place with the majority choosing to go with the proposal. The risk of hard fork is still there but is reduced as compared to off-chain as there has been a round of consultation and refinement. The surplus maximization is with upgraded chain, **B1**, as [0.5 $< \beta, \gamma <$ 1]. This is also Pareto optimal as compared to the original chain, **B2**. Equation 3.8 gives the surplus payoff for the voters S(V), equation 3.9 gives the surplus payoff for the community and equation 3.10 gives the total surplus payoff S. When we compare the mixed strategy equilibria for cells **B1** and **B2**, we observe that the payoff in **B1** is more than in **B2**.

- If after the voting, post testnet round, the majority chooses to remain with the original proposal, there is a possibility that the upgraded proposal will be payoff maximizing because of vocal minority with intense preference can convince more **C** members to go in for the upgraded chain $\gamma/ > \gamma$, thus increasing the total community payoff. The risk of hard fork is there, based on proportion of **C** members who prefer coordinating to maximize payoff, when compared



Voters (V)	Community (C) Upgraded Chain	Community (C) Original Chain
Accept (β, λ = 1)	A1 S(V), S(C)	A2
Accept (0.5 < β, λ < 1)	B1 β S(V), γ S(C)	B2 (1-β) S(V), (1-γ') S(C)
Reject (0 < β, λ < 0.5)	C1 β S(V), γ S(C)	C2 (1-β) S(V), (1-γ') S(C)

Figure 3.8: Payoff Matrix for On-chain Governance

to those who wish to go with the majority opinion. As γ' increases more members shift to upgraded chain thus neutralizing the majority vote. Equation 3.14 gives the surplus payoff for the voters S(V), equation 3.15 gives the surplus payoff for the community S(C) and equation 3.16 gives the total surplus payoff S. If S >0 majority will move to the upgraded chain as seen in equation 3.17. If S <0 then the majority will stay on the original chain as seen in equation 3.18.

$$S(V) = S_{\text{Yes}} - S_{\text{No}} = \beta k S_V - (1-\beta) k S_V = (2\beta - 1) k S_V < 0 \tag{3.14}$$

$$S(C) = S_U - S_O = \gamma' n S_C - (1-\gamma') n S_C = (2\gamma' - 1) n S_C > 0 \tag{3.15}$$

$$S = (2\gamma' - 1) n S_C + (2\beta - 1) k S_V \tag{3.16}$$

$$S > 0 \text{ if } \quad (2\gamma' - 1) n S_C > -(2\beta - 1) k S_V = (1 - 2\beta) k S_V \tag{3.17}$$

$$S < 0 \text{ if } \quad (2\gamma' - 1) n S_C < (1 - 2\beta) k S_V \tag{3.18}$$

3.6 Application of the Proposed Mathematical Formulae to Real Data

We use Ethereum data to verify our proposed mathematical formulae for prediction of optimal strategies. Ethereum has off-chain governance and after the DAO hack there was a proposal to upgrade the chain in 2016. Major mining pools, amounting to 54%, supported the decision by voting 'Yes' making $\beta = 0.54$ [5]. This scenario corresponds to the 2nd row of the evaluation matrix in Fig. 3.7 with cells B1 (upgraded chain) and B2 (original chain). As per our analysis in subsection 3.5.3, the risk of hard fork exists. However, cell B1 represents a Pareto optimal condition with surplus maximization existing with the upgraded chain, where the payoff of B1 is more than B2 as validated by equations 3.8, 3.9 and 3.10. This will result in the community moving to the upgraded chain (B1). As it was witnessed, a decision was taken by the Ethereum community to go for the protocol update and this resulted in a split in the community C, creating the hard fork Ethereum (upgraded chain). The present day metrics of the upgraded chain (Ethereum) [6] and the original chain (Ethereum Classic) [7] is a validation of our predictions in equations 3.8, 3.9 and 3.10 indicating that the payoff is more with the upgraded chain (Ethereum), where the majority of the community moved to.

3.7 Conclusion

In this chapter we analyzed the position of blockchain governance in the hierarchy of Institutional governance to derive a formal structure for blockchain governance. The chapter viewed blockchain governance from the dimensions of IT governance and then analyzed one dimension of IT governance, namely decision-making process as in the form of voting on a new blockchain improvement proposal, by using Nash equilibria to predict optimal governance strategies. The objectives of the governance process may vary with the blockchain platform, its community composition and business logic. A game theory simulation of the respective strategies of the players was used in an attempt to define

[5] Quentson , A. (2016). https://www.ccn.com/miners-vote-overwhelmingly-support-ethereums-hardfork/, accessed April 22, 2020.

[6] CoinMarketCap. (2019). Ethereum (ETH). https://coinmarketcap.com/currencies/ethereum/, accessed December 15, 2019.

[7] CoinMArketCap. (2019). Ethereum Classic (ETC). https://coinmarketcap.com/currencies/ethereum-classic/ratings/, accessed December 15, 2019.

the most optimum scenarios based on choices made by the voters or the broader community. The chapter, through an analysis of the payoff matrices, proposes mathematical formulae that can predict the occurrence of a hard fork on acceptance/ rejection of a new proposal as well as give an indication whether the majority of the community will move to the upgraded chain or stay on the original chain. We tried to maximize the payoff for the community while steering them to desired outcomes in our analyses and it was observed that a split in the community through a hard fork diminishes the payoff. Off-chain governance mechanism tries to avoid the potential loss of payoff through an inclusive voting process while on-chain includes a pilot testing with an inclusive voting process. On-chain provides an added opportunity to change the value of γ and hence can be concluded as a better governance proposition.

"What's in your hands I think and hope is intelligence: the ability to see the machine as more than when you were first led up to it that you can make it more."

Alan J. Perlis

4

Management Plane for Smart Contracts

The complexity of blockchain technology poses many challenges and foremost amongst these are monitoring and management of blockchain-based decentralized applications. This chapter discusses a novel system to enable management operations in smart contracts. We design, implement and evaluate this novel system, a key aspect of which is that it facilitates the integration of these operations through dedicated 'managing' smart contracts to provide data filtering as per the role of the smart contract-based application user. Evaluation of the overhead costs of such data filtering operations after post-deployment analyses of five categories of smart contracts on the Ethereum public testnet, Rinkeby is conducted. We also build a monitoring tool to display public blockchain data using a dashboard coupled with a notification mechanism of any changes in private data to the administrator of the monitored decentralized application.

4.1 Introduction

Ethereum differs from Bitcoin in being a blockchain platform on which decentralized applications can be built. It offers the service of smart contracts, which are autonomous agents that can replicate the function of legal contracts amongst other advantages [1]. Our analysis of a dataset of 811 Ethereum smart contracts [14] shows that 80% of them have limited code complexity and very low manageability functions. Our analysis of already deployed smart contracts revealed that they had very few to none authorization and manageability functions. Smart contracts form the base of decentralized applications, which might function as products or services for mass usage. IBM is noted to have first used the acronym **RAS** (Reliability, Availability and Serviceability) to describe the robustness of its products. **M** was recently added to make the acronym **RASM** to signify the essential role **manageability** plays in supporting system robustness by facilitating many dimensions of reliability, availability and serviceability [2].

In this chapter, we provide a novel system to resolve two critical manageability issues present in the use of smart contracts in Ethereum and decentralized applications, Dapps. These are data-filtering and monitoring. To the best of our knowledge this work is the first attempt to design, develop, implement and evaluate a working management plane for smart contracts. The implemented data management templates and their associated monitoring tool can be customized and used with any smart contract or Dapp in Ethereum. We mainly developed a method, associated with monitoring operations, where access of data as per role can be changed dynamically through another managing smart contract (henceforth referred to as **MSC**). The employed design is for the monitoring and data-filtering of one smart contract (henceforth referred to as **PSC** for *Primary Smart Contract*) but can be extended to multiple PSC's being managed and monitored by one MSC. The monitoring tool and the templates have been tested on multiple smart contracts from different categories on the Ethereum public testnet, Rinkeby to evaluate the cost of implementing data-filtering and the latency in monitoring.

The remainder of this chapter is organized as follows. Section 4.2 presents the motivation and

[1] Ethereum GitHub. (2014). Whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper, accessed April 1, 2018

[2] Radle, B. What is RASM?, http://www.ni.com/white-paper/14410/en/

the problem statement of this work. In Section 4.3, we detail the design overview of the proposed management plane. The implementation of the management plane which comprises of solidity code for a MSC template and a shell script for sending message calls to blockchain as a part of monitoring script have been elucidated in 4.4. Results of the experimental evaluation of data-filtering and the developed monitoring tool have been analyzed in Section 4.5. Discussion on the results is done in Section 4.6. Related work is highlighted in Section 4.7. Conclusion and future work are drawn in Section 4.8.

4.2 Motivation and Problem Statement

A smart contract is a program that resides and runs on the blockchain where its correct execution is enforced by a consensus protocol. It relies on a programming language provided by the blockchain platform to encode its operations and the ways to handle user transactions. It can implement a wide range of applications including gaming, financial, notary or computation [14]. The main platform for implementing smart contracts is Ethereum, where the programming language used is Solidity [3]. Each compiled smart contract is stored in the blockchain and executed by the Ethereum virtual machine (EVM) running on the network nodes. Each operation in the EVM consumes **gas**. Gas is the metering unit for the use of Ethereum and helps in the calculation of fees in Ether per operation. A Solidity based smart contract is composed of a set of functions which are invoked by the contract users by sending transactions to the blockchain to validate their effects by the network. To better understand how Solidity contracts are written, we have analyzed the dataset used by Bartoletti et al [14] where they identified 811 contracts available on the blockchain explorer (*http://etherscan.io*). We focus on the distribution of number of functions per contract and how many contracts applied authorization to restrict the execution of a function according to the caller address. When analyzing the authorization in each contract, we only counted the number of functions having a solidity modifier matching the regular expression: $m$odifier $[o|O]nly$. Figure 4.1 depicts the empirical cumulative distribution function (ECDF) of the number of functions per smart contract in the overall dataset and

[3] Ethereum. (2020). Solidity Documentation. https://solidity.readthedocs.io/en/develop/, accessed February 3, 2020

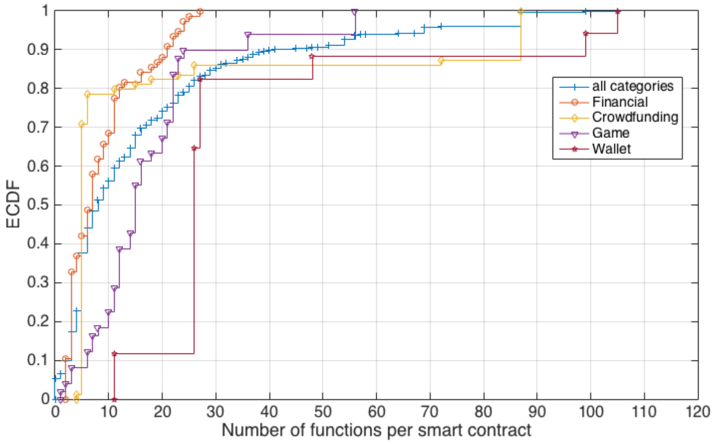


Figure 4.1: Distribution of number of functions per smart contract.

also by category. We observe that around 80% of smart contracts have a number of functions less than 30. In financial and crowdfunding categories this number is around 10 functions. Smart contracts are thus less complex and their number of functions is lower compared to traditional applications.

Figure 4.2 depicts the empirical cumulative distribution function (ECDF) of the number of filtering functions per smart contract in the overall dataset and also by category.

Overall, the number of authorization functions per smart contract is low. The number is lower than 2 for 80% of contracts. We mainly observe that already deployed smart contracts have a low manageability and authorization functions. This analysis and observations motivate our work to provide a management plane able to enforce access control and monitoring operations in smart contracts with an efficient cost.

4.3 Design Overview of the Management Plane

Our goal is to design a management plane to facilitate data-filtering and monitoring services to both blockchain-based applications employing smart contracts and for direct usage of smart contracts. We apply our design, implementation and evaluation of the management plane on the Ethereum platform due its popularity with an increasing number of deployed smart contracts compared to other

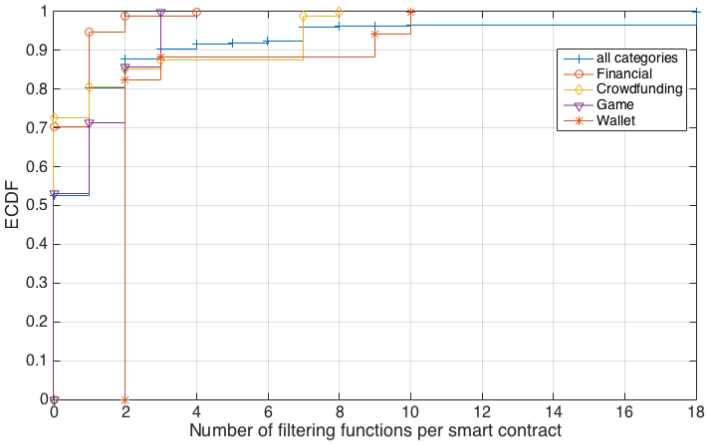


Figure 4.2: Distribution of number of authorization functions per smart contract.

blockchain platforms. Figure 4.3 depicts an overview of the elements of the architecture used to implement our management plane and its instantiation within the Ethereum platform.

The management plane relies on two components namely a **data-filtering service** and a **monitoring service**. The **data access manager** interacts with the data-filtering service to update the access of a certain user to the data manipulated in the PSC. This is accomplished through a management interface relying on smart contracts, denoted as MSC's, to make the update operations. The management interface maintains the connection with the PSC whose data access control is being managed. The monitoring service collects and displays at periodic intervals the monitored data through a dashboard to the users. This is facilitated through a monitoring interface by way of which interaction with the PSC that is being monitored takes place. Both the data-filtering and monitoring service can be implemented to work for single and multiple PSC's as shown in Figure 4.4.

In a one-to-one relationship as depicted in Figure 4.4 the smart contract-based management interface has dedicated MSC's to manage data access in individual PSC's. Each MSC manages one PSC. Similarly the monitoring interface has one monitoring script to monitor data in a PSC.

In a one-to-many relationship the monitoring interface has a single monitoring script to support multiple PSC's as shown in Fig. 4.4. In such a relationship, the smart contract based managing inter-

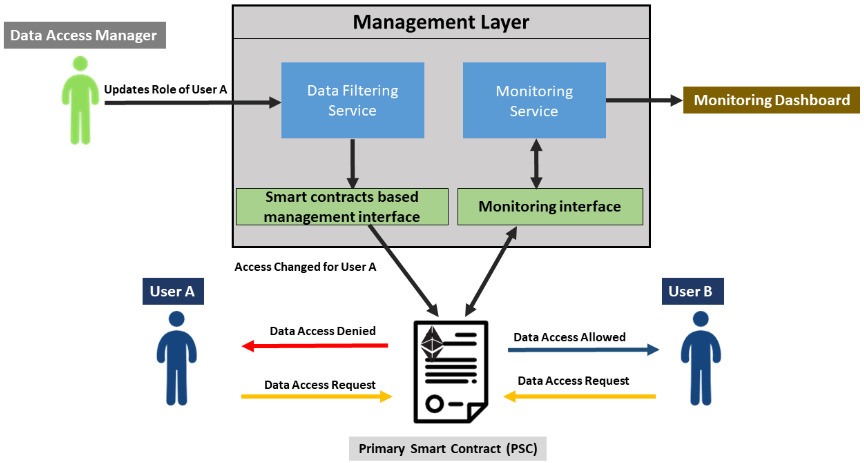


Figure 4.3: Functional Architecture of the Management Plane.

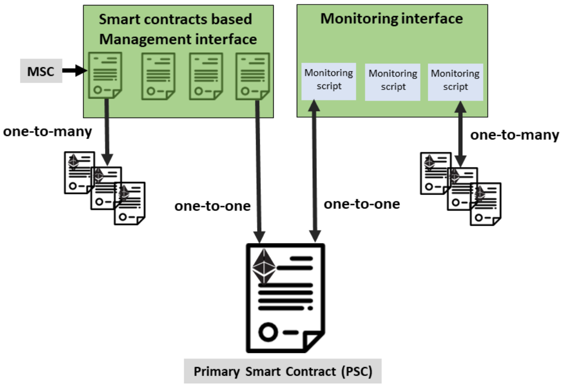


Figure 4.4: Interaction relationships, one-to-one and one-to-many, between management services and deployed smart contracts.

face has a single MSC managing data access in multiple PSC's.

A PSC without a MSC can be extended to include management operations but it would need to be managed separately from other PSC's deployed by an organization, for example. Our developed management plane offers the service of managing multiple PSC's through a single MSC and our cost analysis reveals that this strategy not just implies more management ease but is more cost effective too as seen is Table 4.2.

4.3.1 Data-Filtering Service

A first service that we have designed in the management layer is an authorization mechanism to allow or deny access to data available in smart contract. This data-filtering service is provided through a smart contract based management interface consisting of the MSC's. The PSC is extended to include management operations. These management operations are managed by a MSC in the smart contract based management interface through a **Data Access Manager**. The deployed address of the PSC is provided in the MSC whereas the account address of the Data Access Manager is provided in the PSC. The Data Access Manager is responsible for managing the access of data as per the role/ ID assigned to the application/ smart contract user through the management operations. The Data Access Manager can update the role/ ID of any user at any given moment of time restricting or permitting data access thereby.

4.3.2 Monitoring

The second designed management service is a monitoring mechanism to collect data from a PSC that could be offered through dashboards to an administrator. The monitoring service employs a monitoring interface that comprises of monitoring scripts as depicted in Fig. 4.5. These scripts monitor the changes in data in the PSC and display the real time values to the users through a dashboard. Changes in private data are sent as email notifications to the administrator of the PSC. The changes in data are displayed at periodic intervals, *e.g.* every 10 seconds. The polling frequency can be adjusted depending on the number of users of the PSC or the application and its popularity. The PSC was extended to include monitoring operations as per need. Latency and code overhead to include the monitoring operations was observed, subsection 4.5.2.

4.4 Implementation of the Management Plane

The implementation of the data-filtering service was done in the blockchain itself where the MSC is deployed referencing the deployed address of the PSC. The PSC was extended to include management operations to interact with the MSC. Solidity programming language was employed for programming the MSC and extending the PSC with management operations. The account address of the Data Access Manager was provided in the MSC to restrict updating of access control by non-authorized blockchain users. An option to change the Data Access Manager was also given. The programming code in solidity for a basic MSC is shown in Listing 4.1 and can be used as a template to develop further more customized MSC. Listing 4.1 shows a *secondary* MSC that manages the *primary* PSC extended with the management operation ***updateID***.

```
pragma solidity ^0.4.6;

contract Secondary{

 function updateAccess(uint ID, uint roleno) {
     address Primary=0x692a70d2e424a56d2 c6c27aa97d1a86395877b3a;
     Primary.call(bytes4(keccak256("updateID(uint256,uint256)")),ID,roleno);
       }
}
```

Listing 4.1: Solidity based template of a Managing Smart Contract (MSC)

The implemented monitoring service relies on monitoring operations available in the PSC and a set of external scripts that interact with it to collect the data. *Geth* is the command line interface for running a full Ethereum node. Ethereum provides a JavaScript Console to interact with the blockchain. This JavaScript console is a REPL (Read, Evaluate and Print Loop) exposing the JSRE (JavaScript Runtime Environment). A monitoring tool was programmed to interact through the JavaScript console to the target deployed PSC. The monitoring tool accesses the JavaScript console through a non default IPC endpoint. The *geth attach* command is used in our prototype to achieve the above. The monitoring tool is implemented through a series of shell scripts. The tool sends message call transactions to the Ethereum network, which are directly executed in the EVM but without effect on the network. Since the call transaction does not broadcast or publish anything on the blockchain, there is no consumption of ether. It is a read-only function that causes no state changes. The return values of these calls are displayed to the application users or the users of the smart contract through a dashboard. Only the public data is displayed through the dashboard whereas the private data, on any change, is notified by an email to the administrator of the smart contract.

```bash
#!/bin/bash
geth attach ipc:/home/testnet/.ethereum/rinkeby/geth.ipc << EOF | grep "RESULT: " | sed "s/RESULT: //"
primary = web3.eth.accounts[0];
var MyContract = web3.eth.contract(ABI);
var MyContractInstance = MyContract.at("0x7605a157861e56be8b67c09dfd5f93f3f3ac0995");
txhash=MyContractInstance.MinDeposit.call({from: web3.eth.accounts[0]});
console.log("RESULT: " +txhash);
EOF
```

Listing 4.2: A monitoring Script to interact with a Primary Smart Contract (PSC)

The code of a shell script making calls to the blockchain to monitor data is shown in Listing 4.2. This shell script first employs **geth attach** to connect to the Ethereum public testnet, Rinkeby to allow for further interactions between the script and the blockchain. The account address to be used for sending message calls is first defined and then the address of the deployed smart contract is given. Application Binary Interface (ABI) of the deployed smart contract is needed which is passed on to the script. We only indicate **ABI** instead of listing the ABI of the smart contract for easier reading of the script. Thereafter a message call **MinDeposit** is sent to Rinkeby and the result displayed in console.

4.5 Experimental Evaluation

A prototype of our management plane for Ethereum based smart contracts is developed using Solidity programming language [4], JavaScript API [5], bash, SMTP [6] and HTML language. The smart contracts under study were deployed and tested on the Ethereum public testnet, Rinkeby [7].

4.5.1 Data-Filtering

We validated and evaluated the management operations on 5 categories of smart contracts, which are **finance**, **game**, **notary**, **library and utilities** and **wallet**. A smart contract was chosen from each category and modified to facilitate data-filtering by extending the contract code with management operations. During this phase, we observed that different categories had different management requirements that we will discuss in the next subsection.

Cost Analysis

In order to evaluate the usability versus the overhead associated with implementing data-filtering it was essential to analyze the cost of deployment of the PSC and then the PSC extended with management operations together with the MSC. The MSC is the one that is owned by the *Data Access Manager*. The table 4.1 lists down the various costs as per the category of the smart contract. In **finance** category two smart contracts were analyzed as the first needed very little management operations to be implemented. Similarly in the category **library and utilities** two smart contracts were analyzed and none needed any management operations and data-filtering as per our analysis. Table 4.1 depicts the cost in Ethers and the gas used for one analyzed PSC in each category. Post data-filtering (indicated as **with data-filtering** in Table 4.1) includes the costs in Ethers and gas used for the PSC with implemented management operations and the MSC.

[4] Solidity documentation, https://solidity.readthedocs.io/en/develop/

[5] web3 JavaScript app API, https://github.com/ethereum/wiki/wiki/JavaScript-API

[6] SendEmail man pages, http://manpages.ubuntu.com/manpages/wily/man1/sendEmail.1.html

[7] Rinkeby, https://rinkeby.etherscan.io/

Table 4.1: Cost analysis of data-filtering in 5 categories smart contracts

Category	Smart Contract	Ether	Gas Used
Finance	crowdSale.sol	0.01596964	798482
	with data-filtering	0.02447288	1223644
Finance	SquareEx.sol	0.001607982	1339985
	with data-filtering	0.0113376036	1866480
Game	simpleDice.sol	0.01818752	909376
	with data-filtering	0.0325259	1626295
Library	DateTime.sol	0.01885978	942989
	No data-filtering needed	NA	NA
Library	strings.sol	0.00137306	68653
	No data-filtering needed	NA	NA
Notary	notareth.sol	0.01383504	691752
	with data-filtering	0.02718754	1359377
Wallet	SimpleWallet.sol	0.01192706	596353
	with data-filtering	0.02020668	1010334

A single MSC was developed to manage all the considered PSC's to analyze the feasibility and costs of a one-to-many management approach. A comparison was made between the costs of deploying this single MSC managing 5 extended PSC's with the cost of deploying 5 individual MSC's for each extended PSC. The extended PSC is the smart contract that has been extended to include management operations. The comparison results are depicted in Table 4.2. We observe that both the gas used and cost in ether of using a single MSC to manage 5 extended PSC's was less than the overall cost when using single MSC for managing each of the same 5 extended PSC's.

4.5.2 Monitoring

The monitoring tool was implemented to display the public data of the *simpleDice.sol* PSC deployed on the public Ethereum, Rinkeby testnet. Experimental evaluation of the tool was done by executing

Table 4.2: Cost analysis of management of 5 smart contracts

Management Relationship	Ether	Gas Used
One-to-Many	0.026072	1303600
One-to-One	0.03246534	1623267

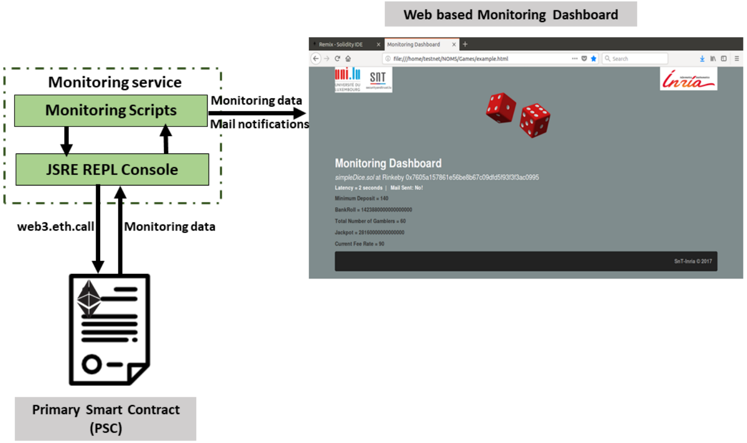
the monitoring script 10 times to monitor PSC data at periodic intervals of 10 seconds. A script was coded to inject data into the PSC at periodic intervals of 5 seconds and this was executed 8 times. Both the scripts were run in parallel. The time difference and also the difference in the number of executions was done to take the mining operation into account, which is not instantaneous in Ethereum. As mentioned before in the previous section, elaborating the design of the management plane *geth attach* was used through the ipc endpoint to interact with Rinkeby through the JavaScript console. Bash script was used to fetch the results of executing *web3.eth.call* [8]. The monitoring script controlled the access of the return values and sent the values to another script, which displayed the return values through a dashboard to the users. A screenshot of the dashboard is shown in Fig.4.5. There are few function calls in the PSC, where the return values are private and any change in them is intimated to the administrator by using SMTP-based *gmail* notifications, whereas the dashboard simply indicates whether a mail was sent to the administrator during this particular cycle of fetching data or not. A demo of the dashboard was recorded [9]. The monitoring tool was implemented for just one PSC but can be extended to any number of PSC's. The basic template that was developed can be applied to any type and any number of smart contracts, on any of the ***Ethereum testnets*** and the main Ethereum network ***Homestead***.

Code overhead

The monitoring tool also records the latency observed in fetching all the public data from the PSC including sending the email notification in case of any changes. The latency would vary with the number of message calls to the blockchain network. In our case the monitoring tool sends 6 message

[8] See 5

[9] Demo of the Monitoring Dashboard, https://youtu.be/kA7A9ysvT28



Monitoring Dashboard

simpleDice.sol at Rinkeby 0x7605a157861e56be8b67c09dfd5f93f3f3ac0995

Latency = 2 seconds | Mail Sent: No!

Minimum Deposit = 140

BankRoll = 1423880000000000000

Total Number of Gamblers = 60

Jackpot = 28160000000000000

Current Fee Rate = 90

SnT-Inria © 2017

Figure 4.5: The components of the monitoring service.

Table 4.3: Code overhead for *simpleDice.sol* smart contract.

Script Function	Lines of Code
Sends Message Calls	16
Monitors Data	37
Displays Data	54

call transactions to Rinkeby, which includes monitoring a single private data for email notification in one cycle. It was observed that the latency for one cycle varies between 5 to 7 seconds. The code overhead in terms of the number of lines of code needed to implement the above is given in Table 4.3. Table 4.3 examines the script used indicating its function. The total overhead from Table 4.3 for monitoring the PSC is **107** lines of code as opposed **16** lines of code for just fetching data through 6 message calls. The code overhead is to give a general indication and there can be some reduction in the overhead if the code is optimized.

4.6 Discussions

Distributed database as in a blockchain pose significant challenges of security, data access, monitoring and configuration issues. The very same issues that are present in centralized DBMS become more complex in distributed databases. The chapter successfully designs, implements and analyzes two crucial components of a management plane namely, data-filtering and monitoring for an application on a distributed network. This is a very valuable initiation towards developing a full-fledged management plane for blockchain and other distributed databases.

Smart contracts are immutable once deployed on the blockchain and no changes can be made in the source code. We have analyzed smart contracts from five different categories. As a result of the analysis it can be concluded that financial smart contracts needed little management operations as the original developers had taken care to include some role-based access to data. Library and utilities needed no data-filtering. In all the smart contracts observed, apart from one, none had the *self-destruct(address)* option. The smart contracts cannot be deemed as complete for mass usage as both role-based data access to allow management operations, monitoring operations as well as control operations to bring about aborting of the smart contract were missing. This makes most of the deployed smart contracts redundant for any practical real world usage except for experimentation. One of the probable reason behind this might be that the smart contracts currently in the blockchain network are limited in the number of users as compared to traditional web applications leading to less focus on implementation by the relatively small community of smart contract developers.

The cost analysis of the management operations that we implemented to provide data-filtering service revealed that smart contracts from the category **Library** needed no management operations as per our analysis. **Wallet**, **Notary**, **Finance** and **Game** needed approximately the same number of functions to implement management operations with the **Finance** smart contracts leading in the amount of gas used followed by **Game**. It was also found through experimental evaluation that a management relationship where a single MSC manages and monitors multiple PSC's is better from an economic point of view in terms of gas usage.

Monitoring of data involves a code overhead and latency that increases with the increase in the number of message calls to the blockchain network, which in turn depends upon the number of functions that return data, being monitored.

4.7 Related Work

In [40] Clack et al. focus on management of the complete lifecycle of 'smart' legal contracts, whereby they study the creation of legal contract templates and their subsequent use between contracting parties. They do not go into analyzing the management of the smart contracts itself, which has been accomplished in this work. In [68], Gervais et al. introduce a novel blockchain simulator to analyze the security and performance of proof of work blockchains like Ethereum. This work differs in being an analysis of a management plane for Ethereum applications employing the use of smart contracts through programmed scripts and developed tools interacting with the real Ethereum public testnet. The work [128] provides a GUI-based tool for users to easily create more secure smart contracts. They also provide a set of design patterns as plugins for developers to enhance security and functionality of the smart contract. Our work is complementary where we provide data-filtering and monitoring templates for developers which can be used for implementing a management plane in applications using smart contracts. In [9] Anderson et al. categorize the Ethereum transactions into currency transfers and contract creations whereas this work deals with analyzing a smart contract in each category from amongst the total categories in which smart contract can be demarcated according to the work [14] by Bartoletti et al. In the latter work, the authors make a quantitative analysis of the usage and programming of a smart contract in Ethereum. In [181] Cook et al. develop DappGuard to monitor incoming transactions for any smart contract it manages with the intent to detect any potential vulnerabilities.

4.8 Conclusions and future work

In this chapter we designed, implemented and evaluated a management plane for both smart contracts and smart contract-based decentralized applications. Two services have been instantiated in this plane which are data filtering for access control and data monitoring of deployed smart contracts. The two services could be applied using a one-to-one or one-to-many management strategies for interacting with the managed contracts. Our evaluation of these strategies regarding Ether fees and the used gas shows that one-to-many has a lower cost than a one-to-one strategy.

As a future work, we are working on the extension of the monitoring service with smart contract-based interfaces to monitor deployed ones. In the present implementation the restriction in data access through a decentralized application can be bypassed on the Ethereum blockchain and we aim to circumvent this in our future work. We are also interested in providing a more seamless instrumentation functions for smart contracts to integrate monitoring operations with little effort from the developers. Finally, we want to investigate further the evaluation of the cost of management while varying different factors including monitoring polling frequencies, number of monitored and accessed attributes, etc.

"Our own information is being weaponized against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold."

Tim Cook

5

Data Privacy in Blockchains

One of the main challenges of the emerging blockchain systems remains to address data privacy. In Bitcoin and similar e-cash systems, privacy is limited to anonymity and addressed by using cryptographic pseudonyms for identification and authentication of parties. Privacy has more breadth in systems maintaining actual data such as medical records or energy meters. This chapter is divided in two units. Unit I conducts a review of recently proposed privacy-preserving blockchains with an analysis their strengths and weaknesses. The unit also highlights research questions related to differential privacy, requiring future investigation. Unit II introduces a novel privacy management plane which integrates differential privacy to query existing relational databases through the blockchain as well as spearheads the use of blockchain for local differential privacy. The distinguishing feature in the latter is that the privacy management plane gives the data owners the right to perturb their data with the desired privacy budget, while in the former it gives the right to the data curator to change the privacy budget dynamically while answering queries through the blockchain. The unit also includes experimental evaluation of the developed privacy management plane and integrates management operations in it through another smart contract. The unit further addresses the issue of GDPR and it's implications in the context of blockchain data, while highlighting the compliance of the proposed implementation.

The units in this chapter are as follows:

1. **Unit I: Privacy-preserving Blockchains** (Section 5). This unit deals with the review of prominent privacy-preserving blockchain platforms and puts forward research questions on the use of differential privacy in blockchain platforms.

2. **Unit II: Management plane for differential privacy preservation through smart contracts** (Section 5.4). This unit introduces a novel privacy management plane which utilizes differential privacy to preserve data privacy while querying relational databases, as well as aids to preserve local differential privacy. The unit also addresses GDPR and highlights the compliance of the proposed privacy management plane.

The work done in Unit I is amongst the first reviews in the domain and Unit II is a pioneer in proposing a privacy management plane that adheres to the guidelines of GDPR.

Unit I: Privacy-preserving Blockchains

5.1 Introduction

Bitcoin spearheaded the development of many blockchain platforms. The new blockchain platforms promise to enhance the original Bitcoin framework by diminishing cryptographic-related energy consumption through mining, incorporation of access control, and supporting the diversity of stakeholders, roles, incentives, and consensus algorithms. Blockchain smart contracts promise to complement and even replace legal contracts by associating scripts to transactions. These contracts are formed of an agreed-upon source code, which is granted automated execution among all the nodes. The current state of the execution is also subject to consensus and stored in the ledger. The emerging technology provides many benefits such as data immutability, transparency, integrity, and auditability, which makes it suitable for innovative use cases in many domains like online voting, IoT and AI [170]. However, emerging interest and recent research in blockchain still have not provided solutions to some fundamental issues like scalability, real-timeliness, security, and privacy, which hinders a wider adoption of this technology.

In this unit, we focus on existing privacy-preserving approaches in blockchain. A review of recent literature indicates that privacy is assigned multiple definitions and viewed from different perspectives. One perspective considers privacy to be equivalent to providing an access control and protection layer of the data, based on tailored encryption. Another perspective considers privacy to be equivalent to blind data aggregation and computation. Techniques from secure multi-party computations such as garbled circuits and homomorphic encryption are deployed as smart contracts to protect users' input and only reveal the final output to the designated party. These directions have their merits but our argument is that privacy-preserving blockchains should be derived from formal definitions of privacy ensuring a strong guarantee such as the differential privacy framework. This matches the point of view

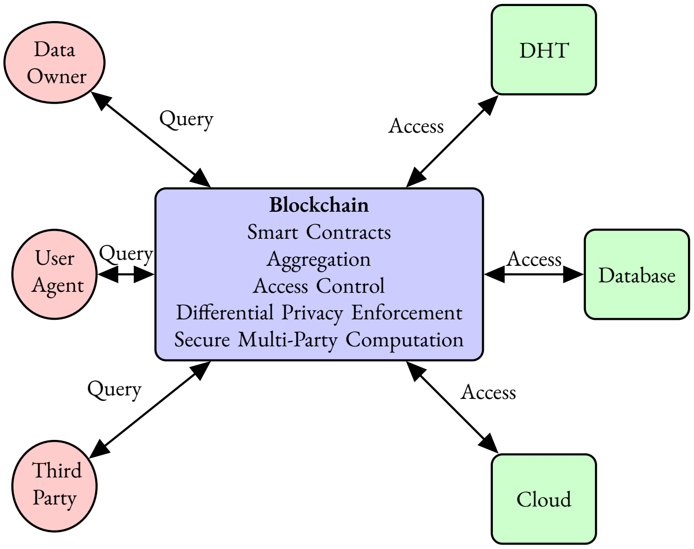


Figure 5.1: High-Level Diagram of a Privacy-Preserving Blockchain

of many contributors, who cited differential privacy as their future work.

A high level diagram depicting the building blocks of privacy-preserving blockchains is depicted in Figure 5.1. The actual data is usually stored off-chain for efficiency. The data is either centralized in the cloud or external databases, or decentralized in a Distributed Hash Table (DHT). Several parties require access to manage the data. For instance, we enumerate data owners, stakeholder applications, and third-parties, who might be interested in an aggregated information.

The rest of this unit is organized as follows: In section 5.2, we study several privacy-preserving blockchains. Section 5.3 suggests research questions for future investigation while conclusion is given in 5.4.

5.2 Privacy-Preserving blockchains

We discuss several blockchains from the literature, which have been announced as privacy-preserving. We describe each framework and provide a brief assessment of its security and privacy aspects. We summarize the properties of these systems in Table 5.1.

Table 5.1: Summary of privacy-preserving blockchains

Blockchain	Application	Aggregation	Access Control	SMC	DP	Assessment
Power Grid	Power Grid	✓	✓	✗	✗	Single point of failure
Ancile	Electronic Health Records	✗	✓	✗	✗	Smart contracts not private
Enigma	General computations	✗	✓	Secret sharing	✗	Malleability; Replay attacks
Dash	Cryptocurrency	✗	✓	✗	✗	Cluster intersection attack
Monero	Cryptocurrency	✗	✓	Additive HE	✗	Temporal analysis
Zcash	Cryptocurrency	✗	✓	Additive HE	✗	Third party trust

5.2.1 Blockchain for Power Grid

A privacy-preserving and an efficient, aggregation blockchain framework for power grid communications in smart communities is proposed in [76].

Description

In this system, each group of users forms a blockchain. In each time slot, a user is chosen at random as the mining node according to the average electricity consumption data. The details are omitted but one can imagine that the users broadcast their measurements in a first round. Thereafter, all the users locally compute the average of all the received measurements. In the end, each user decides whether their measurement is the closest to the average. In this case, the user is responsible for aggregating the data and recording it to the blockchain by submitting a transaction. It is assumed that aggregating the data hides individual contributions and hinders user profiling based on energy consumption profiles. This is questionable from a differential definition of privacy.

A key management center (KMC) is responsible for initializing all the keys in the system. It generates multiple public and private key pairs for each user and takes the public key as the user's pseudonym. The pseudonyms of a group of users are used to construct a Bloom filter. The KMC broadcasts the Bloom filters to their corresponding groups, to be used in membership authentication.

Assessment

Some of the security issues that need to be addressed are as follows:

- The node to aggregate the energy measurements is chosen randomly. This is not sufficient to consider that the chosen node is honest. If 10% of the nodes are malicious, then there is a 10% chance to elect a malicious leader. Usually, blockchains assume 49% of nodes being malicious in the worst case. The scenario where a malicious node claims to be elected should be investigated.

- The Bloom filter is made public. It is easy to break the authentication by brute-forcing an ID that passes the Bloom filter test. Usually, the Bloom filter must be kept secret.

- The generation of all the keys by the KMC is not a good security practice. Usually, a private/public key pair is locally generated and the public key ownership is proved by a certificate. The certificate gets signed by a third and trusted authority.

- The KMC is a centralized, single point of failure, which contradicts the decentralized nature of a blockchain.

- When viewed from a differential privacy perspective, we are catering to an aggregate query about a database of users (e.g. average, or sum). This is not considered safe without determining the query sensitivity and applying a noising mechanism.

5.2.2 Ancile

Description

Ancile is a framework for access control and interoperability of Electronic Health Records (EHR) [45]. A pool of voter nodes, operated by the government and EHR providers, run a consensus protocol. 51% of the nodes are assumed to have good incentives. The nodes form a permissioned blockchain that plays the role of an access control layer in between patients, EHR providers and insurance companies. Hashes of records and their query links are placed in the blockchain. The patient is considered the owner of the record. Access permissions are granted to other parties through smart contracts. For instance, the patient can change the insurance company by denying access to the old insurer and granting it to the new insurer. The medical record is transferred off-chain through HTTPS from one EHR database to another. Each node is mainly composed of a cipher manager, a database manager, and an Ethereum Go client. Six contracts are proposed to manage and protect the different aspects of EHR.

Assessment

The framework is based on previously proposed cryptographic building blocks, such as proxy re-encryption, network-wide symmetric keys and public/private keys for authentication. The architecture and flow-control of smart contracts are discussed at a high level. A security assessment requires a more in-depth evaluation of the building blocks. In general, the wide span of the system and the interdependence of smart contracts contribute to a large attack surface. The system highlights the importance of differential privacy and mentioned it as future work.

5.2.3 Enigma

Description

Enigma [210, 209] recognizes that blockchains, in their current design, cannot handle privacy at all. The reasons cited include that blockchains have a public and permissionless nature, can only execute fiduciary code with intensive verification, and are not well-suited for heavy computations. Enigma's definition of privacy is inherent to secure multi-party computation (SMC), and secret sharing schemes in particular.

Secret sharing is a threshold cryptosystem, where a secret s is divided into n shares distributed among n parties. The original secret (s) can be reconstructed using any $(t + 1)$ shares $(t < n)$ but not less. Secret sharing have homomorphic properties which allow for evaluating arithmetic circuits. Enigma is designed as a peer to peer network with DHT and secret sharing principles, and interoperability with a blockchain. Blockchain is used as a back-end to store public data, references to private data, and transactions. Blockchain handles identity management, access control and only lightweight computations.

Enigma introduces the idea of a *private contract*. A private contract has public parts which are executed on-chain and private parts which are executed off-chain.

Assessment

Enigma is an ambitious project, still the interoperability aspects are not fully covered and may need further investigation. Some of the design choices in Enigma that can lead to vulnerabilities or potential violations of privacy are:

- Enigma is based on SPDZ for correctness against malicious adversaries. SPDZ comprises of an expensive pre-processing step which uses somewhat homomorphic encryption (SHE) to generate shared randomness. However, homomorphic encryption is known to be subject to malleability attacks, and is not considered IND-CCA2 secure, which is the de-facto security definition. [123].

- The interoperability of two or many peer to peer networks requires complex management, which may allow some attacks such as replay attacks. For example, the authors in [43] discovered a vulnerability in the Helios voting system which works by replaying a voter's ballot or a variant of it. The replayed ballot magnifies the voter's contribution to the election outcome, and this magnification can be used to violate privacy.

- The incentive system of the blockchain (i.e., mining rewards) is different than the incentive system of Enigma (i.e., computational fees), which may lead to unstable or concurrent behaviors. Computational metering does not have cryptographic proofs as in mining rewards.

5.2.4 Dash

Description

Dash is a cryptocurrency that seeks to enhance Bitcoin by providing instant transactions as opposed to the long confirmation times needed by the Bitcoin network. Zero-confirmation, tamper-proof transactions and an anonymous cryptocurrency, preserving the privacy of the user are the characteristic features of Dash.

Full nodes in Bitcoin store the entire blockchain and participants in the network rely on them to get information related to the historical data in blockchain as well get updates about events in the network. Full nodes are servers that run on the peer to peer network and consume a significant amount of resources, resulting in a decrease in their number. Users favor running a light client more, which does not store a copy of the entire blockchain and gets information from the full nodes. However full nodes are very important as they manage the functioning of the Bitcoin network. Dash utilizes a secondary network, *Dash masternode network*, comprising of nodes that ensure high availability and requisite services to the underlying blockchain network to aid in enhancing the utility of the blockchain network [55].

Dash is structured as a Decentralized Autonomous Organization (DAO) governed by masternodes and stakeholders. Masternodes in Dash provide second-tier functions namely, *InstaSend* for instant payments and *PrivateSend* for ensuring privacy of the users during payments. The masternodes also provide governance of the underlying blockchain network. These masternodes receive an incentive of 45% of the newly generated Dash. The privacy feature, PrivateSend offered by Dash is an enhanced implementation of *CoinJoin*, a privacy solution in Bitcoin proposed by Maxwell [1]. In PrivateSend, at least three users pool in their transactions to form one transaction by merging the transactions in the

[1] Bitcoin Wiki. (2019). CoinJoin. https://en.bitcoin.it/wiki/CoinJoin, accessed May 25, 2019.

pool together that sends the coins to freshly generated addresses belonging to the three users. This mixing helps to disrupt the blockchain trail of ownership between the users. The privacy is further enhanced by repeating the procedure and mixing with different participants with the default number of mixing rounds being 2. The mixed coins can then be used for PrivateSend transactions. Masternodes are chosen at random to receive the coins from the users and mix them to form one CoinJoin transaction. The masternodes cannot steal these coins from the users. PrivateSend is optional for the users and comes integrated into the default wallet.

Assessment

PrivateSend comprises of mix transactions that use power-of-10 denominations. Therefore the input to the mixing process precludes a step where the coins are broken into these standard sizes and the PrivateSend transactions spend a mixed set of power-of-10 denominated outputs [99].

Some of the potential vulnerabilities that can make the privacy provided by Dash redundant are as follows:

- Dash users need to trust the masternodes with their transactions for mixing. This implies that the masternodes are aware of the wallet addresses being used and the transactions are not completely private. Duffield and Diaz have suggested using masternode blinding via a relay system [55], where the user initially does not send the transactions to the mixing pool but contacts a random masternode, who in turn sends the coins to be mixed to another masternode. This is also susceptible to leakage of privacy because if the masternodes collude together then they can reveal the wallet addresses being employed for the mixing.

- Some masternodes are owned by users who are conducting the transactions and many masternodes appear to be run by virtual private servers, which can be easily compromised.

- It is optional to use mixing, which requires both time and paying of a modest fee. Thus not all users go for PrivateSend transactions. The trail of ownership is disrupted on the blockchain during mixing but the history of mixing is still available.

- Koldner *et al.* exploited the weakness of mixing in PrivateSend transactions to prove that Dash is susceptible to the cluster intersection attack, whereby the mixed coins were successfully linked to the cluster of wallet addresses that held the coins before mixing [99].

5.2.5 Monero

Description

Monero is an implementation of CryptoNote, which is an application layer protocol that supports decentralized currencies [168]. CryptoNote technology relies majorly on the cryptographic primitive called *one-time ring signature*, derived from the work based on *Traceable ring signature* [66]. It helps to provide fully anonymous transactions adhering to both untraceability and unlinkability criterion of an ideal electronic cash [146]. Monero uses EdDSA [18] as the base signature scheme with the transaction structure similar to that of Bitcoin. The difference from Bitcoin in the model adopted by Monero being that the sender generates a one-time public key based on the recipient's address and some random data. An incoming transaction for a recipient is sent to a one-time public key, and not a unique address, with the recipient using his unique private key to recover the funds. The use of stealth addresses as above hides the actual address of the recipient. The owner of a stealth address uses two key pairs instead of one to generate a unique address every time it is used. The recipient can then spend the funds using a ring signature, while keeping his ownership and spending details anonymous [168].

A Monero ring signature is composed of the user spending the funds, combined with the past transaction outputs drawn from the Monero blockchain. This combination serves as the inputs of a new transaction and it is envisaged to be difficult for an observer to know the true input, as all the inputs appear to be equally likely to be the output being spent in a transaction. Thus, the origin of the transaction is masked by making all inputs indistinguishable from one another using the ring signature.

The ring signature scheme employed in Monero creates an avenue for a user to double-spend his funds since verification of the user cannot be accomplished in a ring signature transaction. The resolution for this is the usage of key images by Monero. A key image is a cryptographically secure key generated from the output of a transaction being spent. It is a one-way function of the one-time private key of the actual user spending his funds and is a part of every ring signature transaction in Monero. It is not possible to recover the public key from the key image to identify the actual signer. Monero blockchain stores a list of all the key images of spent transactions, which helps in verification to ensure that double-spending does not take place.

Assessment

Some of the potential flaws that have breached and can make privacy on Monero subject to infringement are as follows:

- The privacy in Monero functions by hiding the actual coins being spent with other coins, called *mixins*, that have already been spent in older transactions. An already discovered privacy flaw was that Monero permitted the feature of privacy as opt-out in the beginning creating the grounds for future identification of actual coins from the older mixins. Since its release Monero has undergone several changes to update its privacy and provide additional features. However, any security flaw that is discovered works retroactively revealing older private transactions from the immutable record of the blockchain. The presence of 0-mixin transactions reduces the untraceability of other transactions with mixins.

- Monero mixins are sampled in a way that they are easily revealed by their age distribution. Temporal analysis correctly identified the actual coins with 80% accuracy over all transactions, with one or more mixins, as usually the ”newest” one [136].

- Online anonymous marketplaces like AlphaBay supported Monero for monetary transactions but they remain subject to transaction graph analysis. AlphaBay’s API was compromised twice, which revealed thousands of private messages and a list of usernames ultimately leading to its closure for involvement in cybercrimes.

5.2.6 Zcash

Zcash is a decentralized anonymous payment scheme that enhances the Bitcoin protocol by providing *shielded* payments secured by zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs). Additionally Zcash attempts to resolve the issue of mining centralization by the use of Equihash [19], a memory-hard proof of work algorithm based on the generalized birthday problem [22]. Zcash is a fork of Bitcoin that ensures the accuracy of the transactions keeping the sender, recipient and the value private, while using the Bitcoin codebase.

Value in Zcash can be either *transparent* or *shielded*. Transactions with *transparent* value work as the transactions in Bitcoin with similar privacy properties. Transactions involving *shielded* value are carried by *notes*. *Notes* specify an amount and a *shielded payment address* as the destination to which the amount is sent to. *Notes* can be spent by using a private key, known as *spending key*. Each *note* is associated with a *note commitment*, which when spent reveals a nullifier. The note commitments and nullifiers are stored as hashes on the blockchain. So, no information is revealed about which nullifier belongs to which note commitment. Additionally, it is infeasible to correlate the note commitment with the associated nullifier without knowledge of the spending key. Note commitments are the shielded equivalents of unspent transaction outputs (UTXO) in Bitcoin. When a note commitment is spent, then the sender reveals the nullifier, which is the hash of a secret number from an existing unspent note commitment and provides a zero-knowledge proof as evidence that they are authorized to spend the note commitment.

The recipient can choose to be private or transparent and as per the choice, the sender can choose the transaction to be conducted and the recipient address to be used, as a user has two payment addresses, associated to transparent or shielded transactions and receives funds accordingly. The zero-knowledge proof ensures that for each note, a note commitment exists and the nullifier for it is computed correctly. Additionally it ensures that there is no collision between the nullifier of one note with that of another.

Assessment of Privacy: Vulnerabilities

Zcash transactions are not private by default as it permits four different kinds of transactions namely public, sender private, recipient private and the entire transaction, including transacting entities, private. The users need to expend more effort for shielded transactions and as per design Zcash inculcates more computational work by the sender minimizing the time and effort required for the verification process. Some of the vulnerabilities in Zcash are as follows:

- Zcash was detected with having an *inflation bug* that made it possible to drastically increase the crpytocurrency to an unlimited amount [2]. Anyone who had access to the multi-party computation script, which is used to set up the privacy features in Zcash, could create false proofs and inflate the monetary supply by counterfeit cryptocurrency. The reason was attributed to a flaw in the underlying mathematics governing zero-knowledge proofs and remedial measures were taken much later than the actual discovery because it was envisaged by the Zcash team that cryptographers with the appropriate skills to exploit the vulnerability are very few in number.

- When transactions are broadcasted, the IP address of the sender is exposed to the network. Anybody who is observing can know which geographical region the transaction originated from as well as which transactions in the network belong to this IP address. Zcash node can be run over Tor for obfuscation of IPs but this kind of anonymization layer support should be offered by default with appropriate education to the users who opt for private transactions.

- zk-SNARKs do require third-party trust to generate SNARK public parameters for constructing and verifying zero-knowledge proofs whenever the Zcash protocol is upgraded and zero-knowledge proofs are changed. The generation of SNARK parameters are equivalent to generation of a public private key pair, where the public key is retained and the private key is destroyed. If the destruction of the private key is not accomplished then malicious actors can use it to create verified transactions [3].

[2] Hackett, R. (2019). Zcash discloses vulnerability that could have allowed 'Infinite Counterfeit' cryptocurrency. http://fortune.com/2019/02/05/zcash-vulnerability-cryptocurrency/, accessed May 28, 2019.

[3] Reuters. (2018). Radioactive toxic waste from Chernobyl used to ensure cryptocurrency's security. ht

5.3 Differentially private Blockchain

We have shown that each of the aforementioned blockchains has its own definition of privacy and its own ways to deal with it. For Guan et al. [76], privacy is about data aggregation to prevent user profiling. For Ancile, privacy is about protecting the data by limiting its access to eligible parties. For Enigma, privacy is about computation with strong input privacy guarantees. For cryptocurrency systems such as Dash, Monero and Zcash, privacy is about protecting the anonymity of identities involved in transactions. However, there exists a very important aspect of privacy which has not been sufficiently tackled yet, namely differential privacy.

Differential privacy provides ways for trading-off the privacy of individuals in a statistical database[4] for the utility of data analysis. Differential privacy has a single tuning knob, namely ε, or possibly two (ε and δ). For example, increasing ε means more utility and less privacy. Generalization of differential privacy have also been proposed, for example, Blowfish privacy tries to provide more tuning knobs by introducing policies [82].

Important research questions that need to be addressed are:

- Can blockchain offer access to its transactional data in a differentially private manner?
- Can blockchain play the role of an access control mediator to a statistical database with differential privacy enforcement?
- How smart contracts may help building a differentially private permissioned blockchain?

5.4 Conclusion

In this unit, a review was done of the recent privacy-preserving blockchains together with an evaluation of some of the issues that can potentially lead to a violation of privacy. Many of the blockchain platforms reviewed are not private by default, imposing an additional fee and time at the user's end

tps://www.rt.com/business/417364-zcash-chernobyl-secrecy/, accessed May 28, 2019

[4] The term statistical database means a set of data that are collected under the pledge of confidentiality for the purpose of producing statistics that, by their production, do not compromise the privacy of those individuals who provided the data (https://en.wikipedia.org/wiki/Differential_privacy).

to utilize the privacy feature. Many others require the trust of third parties making the definition of blockchain as ’trustless’ questionable. The blockchain platforms do not provide built-in IP address anonymization techniques leaving the additional work to the users. Monero and Zcash fare better than others, but recent critical privacy flaws have revealed their vulnerabilities too. It can be observed that implementation of privacy is an ongoing process and each subsequent upgrade is providing more resiliency. The unit highlighted the absence of work integrating differential privacy to data-oriented blockchains. Future work was outlined in the context of implementing a differentially private blockchain, that addresses the research questions enlisted in this unit.

Unit II: Management Plane for Differential Privacy Preservation through Smart Contracts

5.5 Introduction

The advent of blockchain in 2008 with Bitcoin heralded a novel era of technological innovation pervading primarily the finance domain. The emerging technology expanded to other domains with the passage of time, like the education, healthcare and the supply chain industry among others. The envisaged utility of the technology was challenged by inherent bottlenecks like scalability, throughput, data privacy and security. The decentralized distributed database when compared to relational databases scores a lower score in not just performance but ease of use, latency and lack of data deletion and updating [33]. The core features that blockchain technology is leveraged upon are a trustless environment, immutability and transparency, which come at the cost of lack of data privacy, among the other listed challenges. The distributed network with no single entity holding an obligation for the entire network has created the need for new regulations with regards to legality of smart contracts, dispute resolution for transactions taking place through the network and even economic uncertainty regarding the status of cryptocurrency as being analogous to fiat money or a digital token. The technology research firm Gartner has called *blockchain privacy poisoning*, which implies insertion of personal data in the public blockchain, as one of the biggest risks facing the organizations as that makes blockchain non-compliant under the European General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). The requirements by both the laws is that the user data be deleted on need in adherence to the *"the right to be forgotten,"* [5]. The immutable feature of the distributed ledger makes it vulnerable to cyberattacks [6] and there exists a need to conceive a model for utilization of blockchain by organizations whereby the design of the decentralized applications on the blockchain makes it resilient to such attacks.

Dash is a privacy-preserving blockchain and Koldner *et al.* proved that it is susceptible to the cluster intersection attack [99]. Monero is another privacy-preserving blockchain that utilizes one-time ring signature scheme, attempting to provide both untraceability and unlinkability, but is subject to temporal analysis [136]. Zcash provides private transactions secured by zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) but were detected as suffering from an inflation bug [7]. In the wake of GDPR, CCPA and the vulnerability of privacy-preserving blockchain platforms there is a need to address the issue of privacy using a formal, mathematical model for data privacy, namely differential privacy. There is a necessity to develop a design mechanism for blockchain usage, where the benefits of the technology do not compromise on data privacy.

In this unit we focus on the design, development and testing of a novel privacy management plane for preserving the privacy of data using blockchain. We use differential privacy as a privacy-preservation mechanism, which is a formal, mathematical definition of privacy ensuring the preservation of privacy during analyses. We utilize Laplace mechanism to perturb the data and additionally we integrate the privacy management plane with a managing smart contract to facilitate management operations in the smart contract of the privacy management plane. We discuss our implementation with respect to GDPR 2016/679, which is concerned with privacy of data in the the European Union and the European Economic Area as well as exchange of personal data outside the addressed region.

The privacy management plane incorporates a decentralized app and a web application. It addresses

[5] Lindsey, N. Blockchain privacy poisoning a new concern in post-GDPR Era. https://www.cpomagazine.com/data-protection/blockchain-privacy-poisoning-a-new-concern-in-post-gdpr-era/, accessed April 6, 2020.

[6] Kenyon, H. Privacy 'Poisoning' cyberattacks pose risk to blockchain. https://www.govtech.com/security/Privacy-Poisoning-Cyberattacks-Pose-Risk-to-Blockchain.html, accessed: April 6, 2020

[7] Hackett, R. (2019). Zcash discloses vulnerability that could have allowed 'Infinite Counterfeit' cryptocurrency. http://fortune.com/2019/02/05/zcash-vulnerability-cryptocurrency/, accessed May 28, 2019.

both global and local privacy providing a mechanism to preserve privacy in the presence of a trusted data curator as well as in the absence of one. We implement and demonstrate that blockchain can be used to preserve global data privacy by providing query results derived from existing databases in a differentially private manner similar to the norm followed in standard differential privacy. The identity of the user querying the database is not relevant with respect to GDPR and the identity of the data owners in the queried relational database is not available publicly. We also depict that blockchain can be used as an untrusted data curator by recording perturbed data values from individuals as in local differential privacy, which can be queried further for data analysis purposes. We also discuss based on our study that permissioned blockchains is the way forward to ensure GDPR compliance. We deploy and test the privacy management plane on the local *Ganache* network and test the smart contracts in the Ethereum testnet, Ropsten, which is available publicly for use at the smart contract addresses given in Section 5.9. The associated cost computations are given in Section 5.10.

The relevant background on differential privacy is given in Section 5.7, which includes a discussion on the levels of privacy addressed by our implementation as well as the Laplace mechanism. The design overview of the privacy management plane is given in Section 5.8, which gives the functional architecture of the privacy management plane. The implementation of the privacy management plane is discussed in Section 5.9, while the experimental evaluation of the developed privacy management plane is highlighted in Section 5.10. GDPR and its implications are discussed in Section 5.11 while the conclusion is given in Section 5.12.

5.6 Related Work

Zyskind et al. construct a data management platform which involves using blockchain to restrict access to data in an off-blockchain storage, with the key to the data stored on the blockchain [209]. Chen et al. propose a decentralized machine learning system, *LearningChain*, which ensures differential privacy [34]. Hassan et al. discuss the privacy issues raised by integration of blockchain with IoT and analyze privacy preservation strategies, including differential privacy, in blockchain-based IoT systems [185]. Yang et al. propose a blockchain-based anonymization process for the data owners while providing the functionality to validate the privacy budget and adapt it to the privacy requirements of the data owners [200]. Dagher et al. proposed *Ancile* for access control and interoperability of Electronic Health Records. They use permissioned blockchain to store the hashes of records and query links and highlighted differential privacy as future work [45]. In the dissertation author's previous work with Nassar, they analyze recently proposed privacy-preserving blockchains and emphasized on the need to implement differential privacy to ensure data privacy in blockchains [107]. The present work differs in proposing a novel privacy management plane, which utilizes smart contracts to store the results of queries on the blockchain using differential privacy. Our work also uses smart contracts to implement local differential privacy giving an individual user, the freedom to determine his privacy budget. In accordance with GDPR, the privacy management plane when used in a permissioned blockchain network, can prevent read access to a data record.

5.7 Background: Differential Privacy

Differential privacy is a formal mathematical definition of privacy, which ensures utilizing data for analysis while preserving privacy [54, 57, 20, 56]. In the present age where data has become a utility, and extensive analysis of medical records and even online activities is being conducted for research purposes, the significance of individual privacy has increased manifold. The access to data while ensuring a strong privacy mechanism to retain both accuracy of data shared within the limits of privacy is crucial [192]. The objective of differential privacy is to ensure that the analyst remains as unaware about any individual in the target dataset post the analysis as he was prior to the analysis. Thus differential privacy ensures that there is no leakage of data at the individual level in the database. Privacy can be expressed according to the following approaches:

1. **Global privacy.** The need for global privacy arises when an organization releases the database of several people or answers queries on the database. This disclosure assumes that that there is a trusted data curator who holds the data of individuals in a database, comprising of n number of rows. A *query*, q, from the query space $\mathcal{Q}$ is a function to be applied to the database. The privacy mechanism, $\mathcal{M}$ is an algorithm that can be expressed as [187]:

$$\mathcal{M} : \mathcal{X}^n \times \mathcal{Q} \longrightarrow \mathcal{Y} \tag{5.1}$$

In equation 5.1, $\mathcal{X}$ is the *data universe* comprising of the rows of data types, where dataset $x \in \mathcal{X}^n$. $\mathcal{Y}$ is the *output space* of $\mathcal{M}$. The privacy mechanism thus, takes in as input a dataset and a set of queries producing an output string, which is expected to provide answers to queries preserving differential privacy. This approach is henceforth referred to as *global differential privacy* (GDP) in the chapter. The privacy mechanism M is said to be *ε-differentially private* if it satisfies the following for every pair of neighbouring datasets x and x' and every query $q \in \mathcal{Q}$, where $x, x' \in \mathcal{X}^n$ [187]:

$$\forall y \in \mathcal{Y}, \mathcal{P}r[\mathcal{M}(x,q) = y] \leq e^{\varepsilon} \cdot \mathcal{P}r[\mathcal{M}(x',q) = y] \tag{5.2}$$

In equation 5.2, x and x' differ by only one row.

2. **Local privacy.** The need for local privacy arises when a user discloses his personal information voluntarily. This disclosure assumes that the data owners do not trust the data curator and add noise to their data locally. The privacy algorithm can be expressed as [42]:

$$\forall y \in Range(\pi) : \mathcal{P}r[\pi(v) = y] \leq e^{\varepsilon}\mathcal{P}r[\pi(v') = y] \tag{5.3}$$

   It is assumed that the user has a private value v_i in some domain D, then the algorithm π is used to add noise to v_i and is sent as $\pi(v_i)$ to the data curator to derive statistical information from it. Equation 5.3 depicts the set of all possible output values in $Range(\pi)$ for any input v and v' for the algorithm π, where $\varepsilon \geq 0$. This algorithm is formally taken as satisfying *ε-local differential privacy* [42]. This approach is henceforth referred to as *Local Differential Privacy* (LDP) in the chapter.

Privacy budget is indicated by ε and it is used to control the output of the algorithms used in a privacy mechanism. The privacy budget determines how private the output of the algorithm is. Smaller values of ε indicate more private data with a loss of accuracy. The value of ε is generally taken to be 0.01, 0.1, 0.5 and 0.8 [89].

Sensitivity determines how much noise is to be added to the results in differential privacy. It depends on how much the output can change on the insertion or deletion of a single row in a dataset.

5.7.1 Laplace Mechanism

The primary mechanisms to add noise in differential privacy are the Laplace mechanism and the exponential mechanism. The parameter noise is related to the privacy budget and the sensitivity. The Laplace mechanism adds perturbation to the data with noise according to the Laplace distribution in a numerical output whereas the exponential mechanism is mainly used when the outputs are non-numerical. In this work, we focused on Laplace mechanism since the dataset we employed for evaluation is mainly numerical. The scale of the noise in the Laplace mechanism is dependent on the sensitivity function, divided by ε [95].

Laplace Distribution.

The Laplace distribution, $Lap(b)$ with a scale b (centered at 0) is the distribution with the probability density function [58]:

$$Lap(x|b) = \frac{1}{2b} exp\left(-\frac{|x|}{b}\right) \tag{5.4}$$

The variance of the distribution is $\sigma^2 = 2b^2$. In equation 5.4, $x \in \mathbb{N}^{|\mathcal{X}|}$, where $\mathbb{N}$ denotes the set of all non-negative integers including zero. The most fundamental types of database queries are numeric queries, functions:

$$f : \mathbb{N}^{|\mathcal{X}|} \longrightarrow \mathbb{R}^k \tag{5.5}$$

Equation 5.5 depicts queries that map databases to k real numbers. The Laplace Mechanism for any function f given in equation 5.5 can be stated as:

$$\mathcal{M}_L(x, f(.), \varepsilon) = f((x) + (Y_1, ...Y_k) \tag{5.6}$$

In equation 5.6, Y_i are random variables drawn from $Lap(\Delta f/\varepsilon)$ [58].

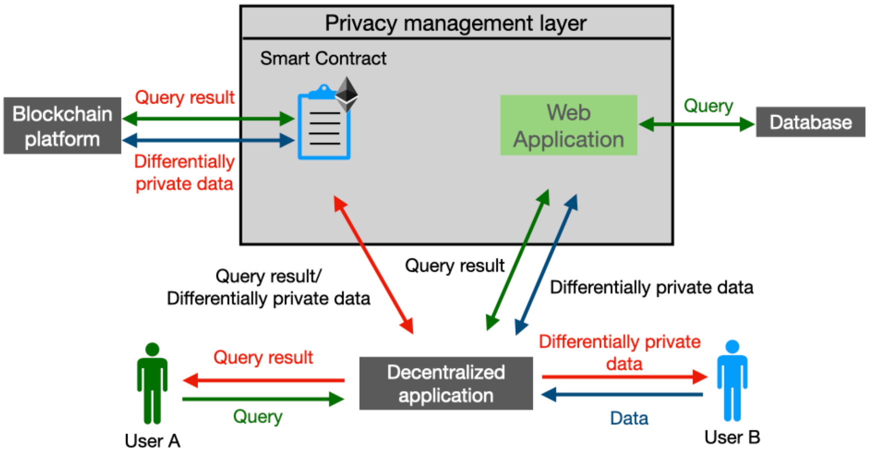

Privacy management layer
Smart Contract
Web Application
Blockchain platform
Query result
Differentially private data
Query
Database
Query result/ Differentially private data
Query result
Differentially private data
Query result
Query
User A
Decentralized application
Differentially private data
Data
User B

Figure 5.2: Functional Architecture of the Privacy Management Plane

5.8 Design Overview: Privacy Management Plane

We developed a privacy management plane to assist in the preservation of both local and global differential privacy. The privacy management plane comprises of a smart contract deployed on Ethereum and a web application. The smart contract is deployed on the Ethereum blockchain network through a decentralized application. The smart contract has functions that cater to both global privacy for organizations owning private databases as well as local privacy for individual data owners. The functional architecture of the data management plane is given in Fig. 5.3.

The mechanism to achieve differential privacy using the privacy management plane is enumerated below:

- Local Differential Privacy: The user inputs the raw data from the frontend of the decentralized app, which is sent by a POST request to a web application, which adds Laplace noise to the raw data depending on the value of ε chosen by the user. The raw data is never stored in the web application. Once the Laplace noise has been added, the skewed data is recorded on the blockchain through the smart contract. This perturbed data is saved by the web application temporarily. This is analogous to users sending data to the data curator by adding noise locally instead of trusting the data curator with their data. The blockchain can function as the data curator in this respect.

- Global Differential Privacy: The user sends a query through the frontend of the decentralized app, which is received by the web application as a POST request. The web application queries the original database, gets the result of the query, adds Laplace noise to it and thereafter returns the result to the decentralized app. The result is also stored on the web application temporarily. The decentralized app records the result through the smart contract on the Ethereum blockchain platform, which can be seen by the user who sent the original query as well as others who have a similar query. In this scenario the algorithm that computes the result of the query and adds noise to it functions as the curator.

5.9 Privacy Management Plane Implementation

The privacy management plane broadly consists of two components, namely the decentralized app, Laplace dapp, and the web application. An overview of the implementation is given in Figure 5.3. The Laplace dapp was developed using the Truffle development environment [8]. The server and web application were developed using Flask 1.1.1 [9] and Python 3.7.3. The smart contract was coded in solidity and was tested on Remix [10] as well as local Ganache blockchain network. The smart contract was deployed and tested on the public Ethereum testnet, Ropsten and is available for access at the Ropsten address *0x13D2E4931C821763145bf18e1f8bE87079F4c84C* [11]. The cost computation was also accomplished on all the testing platforms and shown for Ropsten testnet in Table 5.2. A video depicting the demo of privacy management plane on the local Ganache blockchain network can be accessed from [12].

We used the dataset containing loan details linked to accounts, *loan.asc*, taken from an anonymized dataset of Czech bank [59] to implement and test the smart contract in the privacy management plane.

[8] Truffle Suite. https://www.trufflesuite.com, accessed March 31, 2020

[9] Flask. https://flask.palletsprojects.com/en/1.1.x/, accessed March 31, 2020

[10] Remix - Ethereum IDE. https://remix.ethereum.org, accessed March 31, 2020

[11] Etherscan: Ropsten Testnet. https://ropsten.etherscan.io, accessed: April 7, 2020

[12] Differential privacy enforcement through Ethereum. https://www.youtube.com/watch?v=RtXJHlGqM2U, accessed March 31, 2020

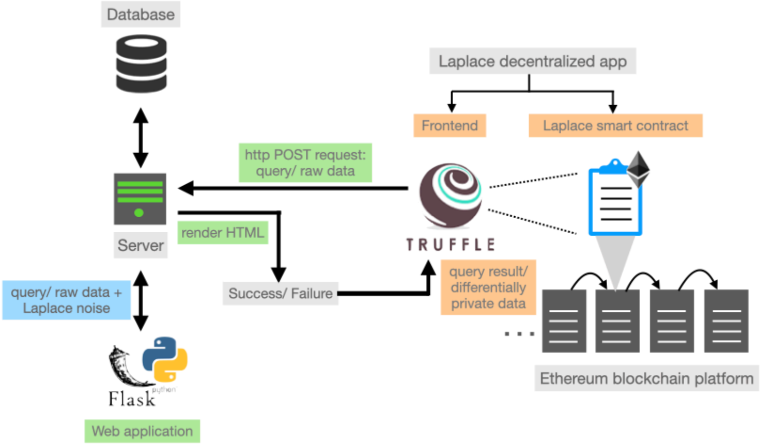


Figure 5.3: Implementation Overview of the Privacy Management Plane

The dataset had columns *loan_id, account_id, Date, Amount, Duration, Payments and Status*. The coded smart contract in the decentralized management plane has functions to cater to recording the query results for this dataset. The differentially private data input by the user to the smart contract to demonstrate local differential privacy incorporates the derivation of the private value from this dataset for the purpose of validation of the implementation. In a practical deployment this private value is with the user himself and not derived from some dataset but prior knowledge is needed on the variable type to be stored on the blockchain. This would assist in coding the smart contract function related to it. A function to answer a simple query by the user to find the *mean* of the column *Payments* or the column *Amount* is given in Listing 5.1.

Relevant code before the indicated function declares a new type through a *struct Query*, which includes 4 fields namely the ID of the query, the selection of the column the user desires the *mean* of, the value of ε and the query result. It must be noted however that in a practical deployment the value of ε should not be known to the user in the scenario of global differential privacy. We have included it in the smart contract to assist in the experimental evaluation of the developed dapp and to demonstrate by our development that blockchain can be utilized to achieve differential privacy. A *mapping* is also declared before the indicated function to ensure that for the ID of the query used as *key* we can access all the fields in the query. The most recent query will have an ID equal to the total number of queries and hence the usage of *numQueries* to access the fields in the query. Lines 7 to 15 comprise of the function to record the query result to find the mean of the desired column in the dataset (see Section 5.10).

```
1  pragma solidity 0.6.1;
2  contract Primary{
3  //code preceding the function
4  mapping(uint=>Query)queries;
5  uint numQueries;
6  //function for simple query
7  function simpleQuery(uint epsilon, uint choiceID, uint result)public{
8      numQueries++;
9      queries[numQueries].queryID=numQueries;
10     queries[numQueries].epsilon=epsilon;
11     queries[numQueries].selection=choiceID;
12     queries[numQueries].result=result;
13 }
14 //rest of the code
15 }
```

Listing 5.1: Smart Contract Function for a Simple Query

The addition of Laplace noise to the data of a user to achieve local differential privacy is depicted in Listing 5.2. The function receives the value of the variable through a POST request and thereafter uses *numpy* to add Laplace noise depending on the value of ε chosen by the user. The perturbed data is written to a file, which is retrieved by the Laplace dapp to record the data on the blockchain.

```
#code preceding the function definition
@app.route('/localdp',methods = ['POST'])
def localdp():
   if request.method == 'POST':
      a = int(request.form['amount'])
      duration = int(request.form['duration'])
      payments = int(request.form['payments'])
      epsilon =  float(request.form['epsilon'])
      scale=1/ epsilon
      s=np.random.laplace(0, scale, 1)
      a=a+s
      duration=duration+s
      payments=payments+s
      f=open("localdp.txt","w+")
      f.write("%d %d %d %f\n" % (a,duration,payments,epsilon))
      return "Success! Local Differential Privacy Achieved"
#rest of the code
```

Listing 5.2: Addition of Laplace Noise to User Data

5.10 Experimental Evaluation of the Privacy Management Plane

We tested the privacy management plane with the dataset, (n=683) containing loan details linked to accounts, *loan.asc*, taken from an anonymized dataset of Czech bank [59]. We deployed and tested the smart contract in Ropsten testnet of Ethereum where the address of the deployed smart contract is *0x13D2E4931C821763145bf18e1f8bE87079F4c84C*. The cost computation for the deployment of the smart contract in Ropsten and the functions used in the smart contract are given in Table 5.2. The cost for the deployment of the smart contract (SC) is $0.11. We coded a function to calculate the *mean* of the column *amount* or the *mean* of the column *payments* giving the option to the user to choose the column. A query to find the sum of either column costs $0.02. We coded a function in the smart contract to cater to a complex query where we find the column *amount* grouped by the columns *duration* and *payments*. The query result comprises of 3 columns with 683 rows. The cost of this query in the blockchain was $18.59. The cost computation has been done using average confirmation time, where the mean time to confirm was approximately 1874 seconds and 125.8 blocks on the day of computation [13].

[13] ETH Gas Station. https://ethgasstation.info/calculatorTxV.php, accessed April 7, 2020

Account	Gas Used	Price (ETH)	Price ($)
SC deployment	570199	0.0006272	0.10662
Simple query	127092	0.0001398	0.02377
Complex query	145656*683	0.1094	18.59
LDP	148103	0.0001629	0.02769

Table 5.2: Cost Computation In Ethereum

In order to aid in our demonstration of the experimental evaluation we used a small subset (n=10) of the entire dataset from Berka [59], which is given in Table 5.3. The given set of records does not indicate the columns *loan_id*, *account_id* and *Date* from the original dataset.

Amount	Duration	Payments	Status
96396	12	8033	B
165960	36	4610	A
127080	60	2118	A
105804	36	2939	A
274740	60	4579	A
87840	24	3660	A
52788	12	4399	A
174744	24	7281	B
154416	48	3217	A
117024	24	4876	A

Table 5.3: Demonstration Dataset

We conducted the following tests through the decentralized app [14]:

- Query to find the mean of the column *Payments* at different values of ε and read the query result from the blockchain. The true mean of the column is 4571.2, which can be verified from the dataset in Table 5.3. The test results are given in Table 5.4.
- Query to find the mean of the column *Amount* at different values of ε and read the query result

[14] See 12

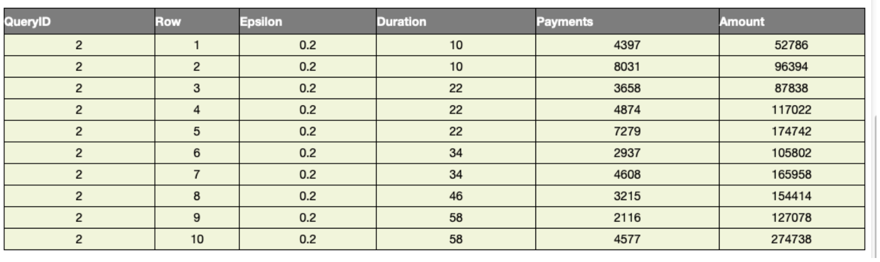
from the blockchain. The true mean of the column is 135679.2, which can be verified from the dataset in Table 5.3. The test results are given in Table 5.4.

- Complex query to find the column *Amount* grouped by the columns *Payments* and *Duration*. The results are depicted in Figure 5.4.
- We simulate the input of private values by 3 users by the input of the raw data from the first three rows of the dataset given in Table 5.3. The data comprises of three private variables from the columns *Payments*, *Amount* and *Duration* through the privacy management plane. They store the perturbed result on the blockchain. The results are read from the blockchain and are visualized through the Laplace dapp in Figure 5.5. The figure depicts the accomplishment of local differential privacy, where the results are stored on the blockchain and the raw data is not stored at any phase of the interaction between the different components of the privacy management plane.

ε	Mean	Column
0.01	4917.78	Payments
0.2	4574.29	Payments
0.5	4571.67	Payments
0.05	135701.82	Amount
0.3	135689.01	Amount
0.7	135679.11	Amount

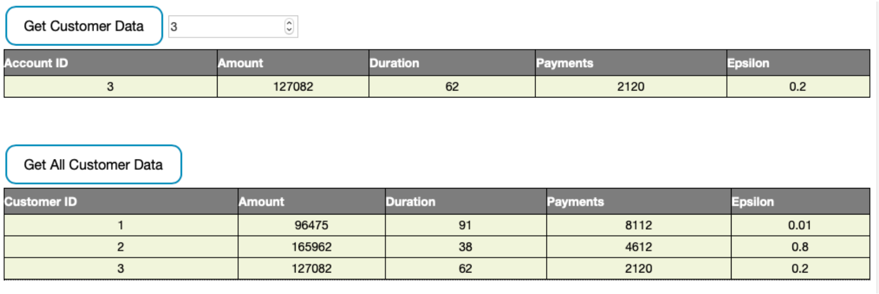
Table 5.4: Simple Query Execution in the Privacy Management Plane

An evaluation of the developed privacy management plane depicts that both global and local differential privacy can be achieved through the blockchain ensuring the integrity of the recorded data. The complexity of the underlying blockchain and the privacy management plane will be hidden behind the decentralized application enhancing the potential usage.



QueryID	Row	Epsilon	Duration	Payments	Amount
2	1	0.2	10	4397	52786
2	2	0.2	10	8031	96394
2	3	0.2	22	3658	87838
2	4	0.2	22	4874	117022
2	5	0.2	22	7279	174742
2	6	0.2	34	2937	105802
2	7	0.2	34	4608	165958
2	8	0.2	46	3215	154414
2	9	0.2	58	2116	127078
2	10	0.2	58	4577	274738

Figure 5.4: Complex query result from the blockchain



Account ID	Amount	Duration	Payments	Epsilon
3	127082	62	2120	0.2

Customer ID	Amount	Duration	Payments	Epsilon
1	96475	91	8112	0.01
2	165962	38	4612	0.8
3	127082	62	2120	0.2

Figure 5.5: Differentially private data read from the blockchain

5.10.1 Integration with Managing Smart Contract

In [106], we developed a management plane to facilitate management operations in smart contracts. The management plane comprised of dedicated *managing* smart contracts, which provided data-filtering as per the role of the smart contract-based application user. The management plane facilitated data-filtering and monitoring services to both blockchain-based applications employing smart contracts and for direct usage of smart contracts. In this work, the local differential privacy implementation poses a scenario whereby a user might revoke his permission to share his perturbed data on the blockchain. Blockchain is a decentralized distributed database, that permits data to be appended but prevents deletion. The data once added to the blockchain cannot be erased. We coded a managing smart contract (MSC) to manage the smart contract in the privacy management plane (LSC) to restrict the read access to a record through the LSC. It will still be possible to read the data from the distributed database of the public blockchain if the adversary is aware of the transaction hash or he goes over all the transactions in the blockchain till he finds the target record. However in an optimally configured permissioned blockchain, the read access can be restricted to only through the smart contracts and then the target record will no longer be available to be read from the blockchain by the users. This can be accomplished by permitting only the users that register through the LSC to have read access. A special identifier can be assigned to each registered user. Permissioned blockchains have an access-control layer built into the nodes and the implemented functionality in this chapter to make a certain data record unavailable through the smart contract will work seamlessly [144].

```
1 pragma solidity ^0.6.1;
2 contract Managing{
3     function updateAccess(uint ID)public {
4       address LSC=0xe7370Fd93bFF00e7Aa98c47665C7DD 18189CF5D2;
5       (bool success, bytes memory data) =    LSC.call(abi.encodePacked(bytes4(
    ↪ keccak256("updateID(uint256)")),ID));
6     }
7 }
```

Listing 5.3: Managing Smart Contract

The updated smart contract, LSC, was deployed and tested on the Ropsten testnet of Ethereum. The address of the deployed smart contract is *0xe7370Fd93bFF00e7Aa98c47665C7DD18189CF5D2*. The managing smart contract was also deployed and tested on Ropsten and the address of the deployed smart contract is *0xE94442bAb9c6500f842E374D7013953ee240630c*. We computed the costs of the additional managing smart contract (MSC) and the updated smart contract (LSC), which incorporated an additional function, *updateID(uint ID)*, to update the ID of the record accessed to revert the transaction in case the record with that ID is queried. The managing smart contract was provided with the address of the deployed smart contract, LSC, and the function to update the target record was made *private* in LSC. The price in $ for the transactions reflects the conversion rate the day the transaction was conducted and is subject to fluctuations. The mean time to confirm the transactions was 1874 seconds while the mean time to confirm in terms of blocks was 125.8 [15]. The managing smart contract is given in Listing 5.3. Line 4 declares the Ropsten address of the deployed LSC while

[15] See 13

Account	Gas Used	Price (ETH)	Price ($)
Updated LSC Deployment	605114	0.0006656	0.11315
MSC deployment	165493	0.000182	0.03094
updateID(uint ID)	22935	0.0000252	0.00428

Table 5.5: Cost Computation for Integration of a Managing Smart Contract

line 5 calls the function *updateID(uint ID)* in the LSC. As a result of this when a call is made to read the data of the customer with the ID passed from the managing smart contract, the blockchain reverts the transaction through the LSC.

5.11 Compliance to GDPR and Implications

The rise of digitising communication forms and societal relationships has positioned differential privacy as an important mechanism to tackle socioeconomic concerns [16]. Although this chapter is targeting computational aspects of differential privacy, and introduces a novel approach to manage differential privacy in blockchains, the societal and economic implications of our privacy management plane are as important to consider. Individuals' attitude on data privacy can vary over time. As Nissim et al. [143] also emphasizes, it is therefore of crucial importance to differentiate among different data privacy attitudes of individuals. The Privacy Act in the United States [91], which dates back to 1974, follows a "Notice and Choice" policy to safeguard data privacy of individuals. The recently introduced General Data Protection Rule (GDPR) [17] in the European Union, however, extends upon this policy, and introduces the rule of "Right to be forgotten" to adopt regulatory mechanism to changing data privacy considerations of individuals, as well as to safeguard data privacy of individuals in the digitized world.

The GDPR is a novel, forward-looking regulatory element of its kind. Even though it is a law of the European Union, its consequences for the global economy are already foreseen [4]. In short, GDPR

[16] Mervis, J. (2020). Researchers finally get access to data on Facebook's role in political discourse. https://www.sciencemag.org/news/2020/02/researchers-finally-get-access-data-facebook-s-role-political-discourse#, accessed February 13, 2020

[17] GDPR.EU. Complete guide to GDPR compliance. https://gdpr.eu, accessed April 3, 2020

establishes clear and consequent rules that govern the transfer and circulation of personal data among different parties, along data supply chains. As such, it declares and provides elementary rules, thus, power for individuals to manage their own data upon their preferences. Most importantly, personal data shall always be erased, once the data owner requests that. Consequently, the decision-making power that is being given implies new regulatory requirements that institutions, data curators need to seriously comply with. The resulting financial penalty is high [18].

As Rieger et al. [162] demonstrates by analyzing an industry-strength, real-life example for blockchain-based data management, that GDPR-compliant application design on blockchains is not a straightforward exercise. The chapter, [162], proposes important recommendations to ensure GDPR-compliant development of blockchain applications. First, for regulatory compliance, personal data shall be stored on systems that it permit rectification and erasure. Second, if a blockchain application processes personal data, private and permissioned approach is desired. The privacy management plane, which we introduce in this chapter is able to adhere to the recommendations and thus provides a practical solution for organizations to use blockchain and remain compliant for the EU law on data protection. The recommendation of erasure can be accomplished by preventing read access to the target blockchain record. Rectification, post accomplishment of erasure, can be achieved by the storage of the updated record on the blockchain.

There exists a crucial design element of our proposed plane. The employment of the privacy management plane to store data on blockchains becomes the function of the differential privacy configurations of the data owner himself. This architectural design strategy provides competitive advantage for any blockchain-based application especially for the European market, as it assures compliance for data curators with GDPR, whereby data can only be shared if the individual, i.e. the data owner allows that to do so. As a novel socioeconomic consequence, the proposed solution actually gives the decision-making power directly in the hand of users to differentiate their own data. Besides the associated operational costs of applying the defined smart contacts which we described in this chapter, the differential privacy choices of data owners might carry potential financial implications for the curators, too. This added power thus might allow data curators to introduce novel data handling practices

[18] Wolford, B. What are the GDPR fines? https://gdpr.eu/fines/, accessed April 3, 2020

for users with direct commercial and socioeconomic consequences.

Individuals' perception on data privacy exhibit a paradox. Athey et al. [11] show, while conducting an experiment with digital currencies, that financial incentives can let individuals' give upon their data privacy. Athey et al. further argue, that a generally provided extra treatment on encryption did not increase privacy-enhancing behavior, but instead potentially reduced it. The privacy management plane, which we introduced in this chapter proposes a technological solution that manages differential privacy with full transparency, and according to regulatory requirements. Our proposed application for safeguarding digital information upon individuals' choices therefore allows corporations to develop blockchain-based applications that not only remain compliant with elementary data protection rules, but also allows developing and applying incentive schemes for individuals to address and to handle their data as an asset. On a longer run, such a mechanism could lead individuals to explore and to understand the valuing fundamentals of their own personal data.

Multiple points of tension have been identified between GDPR and blockchains, and they can be broadly categorized into the following factors as causative agents [60]. The factors responsible for the discord between blockchains and GDPR together with an elaboration on how the privacy management plane resolves them are given below:

1. **GDPR is based on the assumption that for each data point, there exists a legal entity (data controller), who is responsible for the enforcement of the rights of the data subjects under the GDPR.** The developed privacy management plane while ensuring global differential privacy queries a database under the control of a data curator, who is responsible for determining the privacy budget and storing the perturbed query result on the blockchain. In case of local differential privacy, GDPR compliance can be achieved in a permissioned blockchain network, where the legal entity/ entities who employed a permissioned blockchain network for their organization are responsible for the enforcement of GDPR. Their role can be seen in the managing smart contract that was coded to prevent a data record on the blockchain from read access.

2. **GDPR is based on the assumption that data can be erased or modified when necessary in compliance with the legal requirements such as Articles 16 and 17 GDPR.** The data

queried from the database is global differential privacy is off the blockchain and any record can be easily erased or modified. The query result stored on the blockchain will not be impacted significantly by the addition or deletion of a data record pertaining to an individual in the database as per the definition of differential privacy discussed in section 7.2. In case of local differential privacy, we state the significance of the access layer in a permissioned blockchain network for the implementation of the privacy management plane discussed in subsection 5.10.1. The managing smart contract when given the ID of the customer record stored on the blockchain updates the read access to *revert()* the transaction when the ID is invoked using a *call()* preventing the record from being read.

Additionally in achieving global differential privacy the data curator has already anonymized the dataset before Laplace noise is added to the query result through the privacy management plane. In case of local differential privacy, the pseudonymous identity of the individuals revealed through the public-private key pair can be masked by a single or multiple designated blockchain addresses recording data on behalf of the individuals in the blockchain. The cost computation of the transactions conducted by an individual can be negotiated off the blockchain with deduction of deposited fiat money/ cryptocurrency on registration in the decentralized app and input of data through the decentralized app before it is perturbed and recorded in the blockchain for storage.

5.12 Conclusion

In this unit, we introduced a novel privacy management plane which is a pioneering step towards achieving GDPR compliance through the blockchain using differential privacy managed through smart contracts. The developed privacy management plane facilitated data curators to allow queries on their data through a decentralized application with the query results being stored on the blockchain. The storage of query results on the blockchain paves the way for multiple usage of the results without compromising on the integrity of the result and absolves the need for repetition of the same query by others. The privacy management plane also demonstrated the integration of local differential privacy with the individual data owners selecting the level of data perturbation and controlling the privacy budget through a blockchain-based decentralized application. An extension to the privacy management plane integrated the management by another smart contract to prevent a data record stored on the blockchain from being read through the smart contract in the privacy management plane. This enhancement when used in a permissioned blockchain network will ensure the data owner's right to revoke his permission for sharing his data. The developed decentralized application to achieve local differential privacy can be used by organizations to collect perturbed data, giving the users the right to control the privacy of their data with the data being stored off the blockchain if needed and queried in a global privacy context through the blockchain. The implementation is a basic step towards ensuring data privacy and compliance to GDPR. Future work will involve developing a more secure mechanism to access the relational database and add Laplace noise.

"I would not pre-pay. I would invest instead and let the investments cover it."

Dave Ramsey

6

Tokenization of Investment Certificates

Tokenized investment certificates have the potential to expand the investor base to include the average income group, who intend to invest their savings in a deposit for a fixed-term period accruing periodic benefits on it. This chapter is a case study on tokenization of Sukuk, which are investment certificates in the Ethical finance domain, Islamic finance. Sukuk is a financial instrument that provides returns similar to conventional bonds. It has served to cater to the capital requirements of big corporations and governments, while circumventing interest to adhere to the Shariah law. Sukuk can be touted as Shariah-compliant bonds that rank amongst the most successful and the fastest growing financial instrument in the Islamic economy. The sukuk research area is marked by a dearth of quantitative literature, compared to qualitative academic work. This chapter seeks to fill this existing gap, and introduces a novel, exploratory analysis of sukuk tokenization based on a case study. The funding needs of small and medium enterprises remains largely unmet through sukuk on account of the high costs involved, among other reasons. As we show in this chapter, blockchains can aid to lower the cost incurred through the tokenization of sukuk. We highlight some of the key challenges involved in the issuance of sukuk and discuss their resolution using blockchain. We also provide a taxonomy of blockchain applications in finance, with a particular focus on Islamic finance. The chapter reviews different blockchain architectures to assess their viability for tokenization. We conduct a novel case study on sukuk tokenization by implementing a basic smart contract for Sukuk al-Murabaha on Ethereum. The chapter concludes by a conceptual analysis of feasibility concerns, based on a comparison of the conducted cost-benefit analysis of conventional sukuk issuance with tokenization.

6.1 Introduction

The Islamic finance (IF) market will be worth US 3.5 trillion by 2024 [134] and Moody estimations predict an increase in sovereign and supranational sukuk issuance to over $93 billion in 2020 [1]. There exists a strong demand for Shariah-compliant securities from IF institutions. Sukuk offers a stable methodology of financing to institutions looking to diversify their sources of financing. The various projections reinforce the strong foothold of this relatively nascent financial industry. The emergence of new technologies poses a threat to the finance industry and consequently the IF industry is also facing inevitable disruption by a storm of nascent technologies. Blockchain counts as the most potent to cause such a disruption, as the emerging academic literature in finance also argues (see [201]). If the industry does not innovate and adopt to such disruptive trends, then there is a likelihood of a loss of existing client base. The conventional sector is using blockchain to create digital assets like stocks, bonds and land titles e.g. NASDAQ, Chain. The IF industry is also venturing in these areas by creating Sukuk or Islamic bonds on top of the blockchain. The IF sector has witnessed the rise of Sakkex [2] and SmartSukuk [3], which are blockchain-based sukuk issuing platforms. Employment of emerg-

[1] Moody's. (2019). Global sovereign sukuk issuance to recover in 2019. https://www.moodys.com/research/Moodys-Global-sovereign-sukuk-issuance-to-recover-in-2019--PBC_1162325, accessed April 5, 2020.

[2] Sakkex. (2018). Sakkex whitepaper. https://sakkex.io/assets/pdf/SAKKEX-Whitepaper-089.pdf, accessed April 10, 2020.

[3] Blossom. (2019). World's first primary Sukuk issuance on blockchain closes. https://blossomfinance.com/press/world-s-first-primary-sukuk-issuance-on-blockchain-closes, accessed April

ing technologies, in this era of disruption, is an opportunity for the sector to reinvent the established methodologies by incorporating novel technologies to progress ahead of the financial technology startups.

Sukuk has immense potential to fund startups and small and medium enterprises (SMEs). However, sukuk issuance remains confined to large corporations and governments, with the primary target market being large investment funds. The smallest issue is still limited to millions with capital needs of SMEs and startups in the IF domain remaining largely unmet through sukuk. The employment of sukuk for funding SMEs can help to expand the Islamic economy and increase the user base. In [174], Solé describes sukuk issuance and SME financing using a concrete setup of Kuwait and in [152], Patel describes a similar setup for the French market. In these discussions the need for lower transaction costs, transparency and a lack of historic-track record is highlighted, which can be resolved using blockchain.

Sukuk issuance remains plagued with several challenges, the primary being the involvement of multiple intermediaries resulting in both high costs and an increase in the probability of human error. Tokenization of bonds is an application of blockchain technology to lower the various costs associated with the issuance process. Sukuk are Islamic bonds that can also benefit from tokenization by increasing the operational efficiency, cost reduction and enhancing transparency, which is one of the primary characteristics of blockchain. Transparency is also one of the essential attributes that would serve as validation of Shariah (Islamic law) adherence for the masses. Notable organizations have tokenized bonds including World Bank, which launched *bond-i*, which was the world's first bond to be created, allocated, transferred and managed through Ethereum blockchain platform [4]. In 2019 secondary bond trading was enabled on the *bond-i* platform, which was also a pioneer in the world. The Central Bank of China recently issued $2.8 billion of special bonds to fund small and micro-enterprise businesses, using their self-developed blockchain issuance system [5].

12, 2020

[4] The World Bank. (2018). World Bank prices first global blockchain bond, raising a $110 million. https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million, accessed April 27, 2020.

[5] Kuznetsov, N. (2019). China issuing bonds on blockchain is a sign of what's to come. https://cointelegraph.com/news/china-issuing-bonds-on-blockchain-is-a-sign-of-whats-to-come,

The IF domain is characterized by research on sukuk that is largely qualitative rather than quantitative and overall research in sukuk in IF is still underdeveloped [208]. The present chapter seeks to fill this gap. In this chapter, we tokenize Sukuk al-Murabaha using Ethereum through smart contracts to program the necessary conditions like payment frequency, registering investors, automating the periodic payments to the investors while getting the deferred payment amount from the purchaser of the Murabaha asset. We do a cost-benefit analysis of sukuk tokenization with conventional sukuk issuance and conduct a feasibility analysis based on our results. This chapter thus provides an impact-assessment approach for institutions, SMEs and even startups to support the adoption of blockchains for sukuk issuance. As a consequence, our analytical approach allows organizations to prepare for current market challenges in a systemically efficient manner, by understanding the cost and performance consequences of tokenization. The chapter is a pioneer in the IF domain as well as the conventional finance domain.

The rest of the chapter is organised as follows. Related work is given in the chapter in Section 6.2. The chapter gives the requisite background on sukuk in subsection 6.3, including the key challenges and circumvention of some of the challenges encountered during sukuk issuance. A taxonomy of blockchain applications in the financial sector is given in Section 6.4. An assessment of the available blockchain platforms in the context of their viability for usage in tokenization is given in Section 6.5. Tokenization of Sukuk al-Murabaha by means of a basic smart contract is elaborated upon in Section 6.6. The cost-benefit analysis is discussed in Section 6.7. Feasibility of tokenization of sukuk is discussed in Section 6.8 while the conclusion is given in Section 6.9.

6.2 Related Work

In [124], Schletz et al. highlight that both debt and equity instruments can be managed by tokenization, which decreases transaction costs by disintermediation and automation, improves transparency, and thus shortens liquidity requirements. Nam and Yang in [139] observe that blockchain bonds convey information safely between the participating institutions, ensure access to the same distributed ledger through a smart contract and reduce the cost of processing complicated transaction informa-

accessed April 12, 2020

tion by absolving the need for a relay center. Uzsoki in [186] highlights that the financial feasibility increases significantly by tokenizing debt instruments used for financing a project or diversifying a portfolio. Uzsoki also adds that tokenization absolves most of the financial, legal and regulatory intermediaries reducing transaction costs. Sukuk issuance involves compliance to the Shariah and investors request higher transparency depicting the adherence to the Shariah. Zaka and Shaikh postulate that blockchain-based sukuk can enable traceability of assets thereby increasing the investors' confidence [202]. Mohsin and Muneeza in [135] discuss a novel Waqf Sukuk model and emphasize on the usage of blockchain-based smart contracts to make the waqf collection process more efficient and transparent. Muneeza et al. conclude in [137] that blockchain can enable fundraisers in crowdfunding platforms to issue their own shares as a blockchain-based issuance enhances efficiency and reduces costs. HSBC Centre of Sustainable Finance in collaboration with Sustainable Digital Finance Alliance published a report where they conduct a study on blockchain-based bonds, including a green bond, issued by banks up to Q3 2019 and demonstrated efficiency achieved and cost reduction spanning all bonds [88]. Blockchain energizes crowdfunding [137] and blockchain-based crowdfunding in conventional bonds is also a potential support to SMEs and startups. BNP Paribas along with six other European financial institutions has initiated a blockchain platform to permit SMEs to borrow money to their businesses through "mini-bonds" [6]. The present work differs in being a pioneer to conduct a case study on sukuk tokenization using Ethereum. The chapter reviews blockchain platforms for their suitability for tokenization, provides a taxonomy of blockchain applications in IF, provides an algorithm and a basic smart contract for tokenization of Sukuk al-Murabaha on Ethereum. The chapter also conducts a feasibility study based on a comparison of the cost-benefit analysis using conventional issuance and Ethereum sukuk tokenization.

6.3 Sukuk

Sukuk represents the plural form of the Arabic word, Sakk, which means a certificate. Evidence of sukuk can be found as early as 1st century Hijri (Islamic Calendar) and in Imam Malik's 'Muwatta'.

[6] Rizzo, P. (2016). French bank BNP is testing blockchain for mini-bonds. https://www.coindesk.com/french-bank-bnp-testing-blockchain-mini-bonds, accessed April 17, 2020.

In the Umayyad dynasty, the government issued sukuk to public servants and soldiers, which they could redeem at the end of the fixed-term period in exchange for food commodity or sell to others prior to maturity [7]. In 1988, Islamic Fiqh Academy (IFA) passed a resolution 30 (3/4), which defined a sukuk, making it a recognised financial instrument in the IF industry. Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI) defined sukuk as certificates of equal value, representing an undivided share in ownership of tangible assets, usufructs or services [8].

Sukuk, sometimes referred to as Islamic bonds, are also described as Islamic Investment Certificates. However, it must be noted that a bond is a contractual obligation whereby the issuer is obliged to pay bond holders, on certain specified dates, interest and principal. In comparison, under a sukuk structure, the sukuk holders hold an undivided beneficial ownership in the underlying assets. Consequently sukuk holders are entitled to share in the revenue generated by the sukuk assets as well as share in the proceeds of the realization of the sukuk assets. Sukuk are Islamic bonds which behave in practice like any highly-rated conventional bond. However, sukuk should not simply be regarded as a substitute for conventional interest-based securities. The aim is not to engineer financial products that mimic fixed-rate bills and bonds, and floating-rate notes as is largely misunderstood by many, but rather to develop innovative types of assets that comply with Shariah.

A sukuk issuance comprises of an Obligor, asset and typically a Special Purpose Vehicle (SPV) to accumulate taxation benefits and solvency. Issuance of sukuk in global Islamic capital markets is predominantly structured as trust certificates, governed by English law, which generally requires the creation of an orphan offshore SPV in a suitable jurisdiction. This structuring involves the recognition of the concept of trust in the jurisdiction of the Obligor. In other jurisdictions, like those governed under the civil law, this is not the norm and sukuk structuring is being accomplished in accordance with local laws. A pertinent example is that of Turkey, which has legislated the creation of asset-leasing companies acting as SPV to enable the use of sukuk. The essential underlying concepts of sukuk are:

- Transparency and clarity of rights and obligations.

[7] Marifa Academy. (2015). Introduction to Sukuk: Lesson 1. https://www.youtube.com/watch?v=ohimum6V34k, accessed April 23, 2020.

[8] See 7

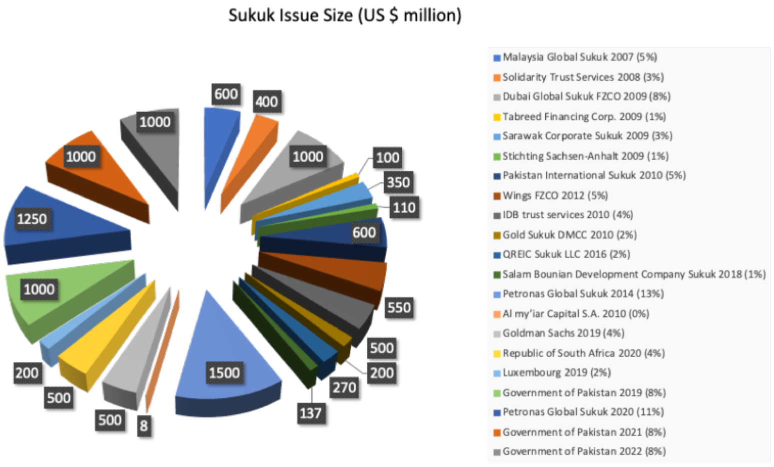


Figure 6.1: Sukuk Listed on Luxembourg Stock Exchange since 2002

- Income from securities must be related to the purpose for which the funding is used, and not simply comprise interest.
- The securities should be backed by real underlying assets, rather than being simply paper derivatives.

Most commonly used sukuk structures replicate the cash flows of conventional bonds. Such structures are listed on exchanges, commonly Luxembourg Stock Exchange and London Stock Exchange in Europe, and made tradable through conventional organizations like Euroclear or Clearstream. Luxembourg Stock Exchange (LSE) is a principal European centre for listing sukuk, which can be done in the Regulated Market, the Euro MTF market or the LuxSE securities Official List (SOL). The securitization vehicles may be used to issue several classes of sukuk. A depiction of Sukuk issuances in Luxembourg since 2002 and their issue sizes can be seen in Figure 6.1.

Key Challenges in Sukuk Structuring

Some of the key challenges that are an obstacle to a greater adoption of this market are as follows:

1. **Slow process.** The documentation process of sukuk issuance is not as fast and efficient as the

conventional bond market, resulting in higher costs.

2. **Decision of the Shariah scholars.** The decision of the Shariah scholars is crucial to any sukuk structuring process and the integration of the Shariah rulings increases the cost of the process.

3. **Lack of standardization.** There are no standards as in the conventional bond market and this slows down the structuring process, adds to the cost and makes the market deployment restricted.

4. **Globally acceptable Shariah standards.** There is a need for Shariah standards to different sukuk structures to have a unified view in the situation of differing Shariah opinions.

5. **Miscellaneous challenges.** There are other challenges like different tax treatments as compared to conventional bonds in different jurisdictions, requirement of a good credit rating and issues related to assets during the transaction life.

Circumvention of Key Challenges

A detailed discussion on the circumvention of all the listed challenges in subsection 6.3 is outside the scope of this chapter. We focus on the listed challenges that can be tackled utilizing emerging technologies like blockchain and highlight the circumvention possible. We sort the circumvention into the following four categories, where all except the last, are addressed in this chapter:

1. **Tokenization.** Tokenization of sukuk using blockchain can help to generate more secure and immutable data while reducing the number of intermediaries involved. Tokenization also facilitates smaller denominations in sukuk issuance potentially extending the benefits of the structure to SMEs.

2. **Smart contract template.** A smart contract template for usage on a blockchain can be provided for different sukuk structuring methodologies in consultation with prominent Shariah scholars. Once the basic template exists, developers can code the IF smart contract with the requisite terms required for a particular sukuk issuance. Validating an enhanced smart contract developed from a basic validated smart contract template, to see if it adheres to a specific

protocol, is faster and easier than documenting a sukuk issuance catering to a specific IF smart contract from scratch.

3. **Automation.** A sukuk issuance involves two different contracts namely, between the Obligor and the SPV, and the SPV and the investors. Multiple smart contracts deployed by the SPV or a third party providing this service, can automate the process and make it more transparent. The automation of periodic payments to the SPV and the proceeds to the investors can make the procedure extremely efficient, transparent and in real time.

4. **Credit rating and market expansion.** Artificial intelligence can be used on the blockchain data relevant to sukuk issuances to develop alternate credit scoring methodologies and expand the market for more organizations to raise capital through sukuk issuance.

The features of blockchain that make it beneficial for the IF industry are thus the following:

1. Transparency
2. Immutable data
3. Absolving the need for intermediaries
4. Smart contracts
5. Decentralized transaction settlement
6. No single point of failure

It is important to mention that blockchain technology is still in its early stages of commercial diffusion. The main underlying reason is that it still suffers from drawbacks, which we discuss in Section 6.8. It is a nascent technology and many providers have come to the forefront offering a blockchain platform. The chapter discusses the implementation of sukuk on Ethereum. Sakkex sukuk issuance is based on Stellar blockchain, whereas SmartSukuk uses public Ethereum. Wethaq's Sukuk platform is based on Corda blockchain platform [9].

[9] r3. (2019). Innovating in Sukuk capital markets. https://www.r3.com/reports/innovating-in-sukuk-capital-markets/, accessed April 24, 2020

6.4 Applications of Blockchain in the Financial Sector

The applications of blockchain are still in the realm of discovery. As our observations conclude, this is mainly driven by the fact that the assessment of performance implications, as well as a solid cost-benefit assessment of such applications remain complex tasks for organizations. To motivate the presence and the role of blockchain applications for finance, and in particular for Islamic Finance, we developed a taxonomy of pertinent financial applications that leverage on blockchains, characterised by their added value and by the markets they target. A more detailed classification with respect to the financial sector can be found in subsection 2.1.3 of Chapter 2. Figure 6.2 depicts the taxonomy, which classifies the applications into the following, nine domains, which emphasizes the application in the IF domain:

1. **Capital markets.** In Islamic capital markets (ICM), sukuk issuance follows a strict Shariah law together in conjunction with the principles followed in conventional bonds with the exception of riba, which can be coded by a smart contract.

2. **Escrow accounts.** In Islamic finance, an application would be where in a Murabaha contract, the buyer would transfer funds to the smart contract account and post transfer of ownership, the smart contract would automatically release the funds to the seller.

3. **Insurance.** The transparency and lack of textual ambiguity in coded smart contracts can prevent legal disputes. There would also be less insurance fraud on account of the contract being pre-programmed according to some specific conditions. Takaful involves peer-to-peer insurance with policyholders supporting each other financially in critical times. Islamic insurance involves management by a takaful operator, where the operator can be replaced by a smart contract managing a pool of policyholders in a permissioned blockchain automating the process and enhancing the transparency.

4. **Loans.** Islamic finance mortgages can reap similar benefits by employing the use of blockchain for granting loans.

5. **Proxy lawyers.** Islamic finance needs lawyers, who can resolve disputes in the Islamic finance domain in the light of the Shariah and similar to the conventional domain, many basic contrac-

tual regulations can be encoded in smart contracts with the violation automatically imposed in case of a deviation from the encoded terms.

6. **Digital ID.** Blockchain-based identity management systems can be used in Islamic finance to make identification and record sharing easier. However privacy issues need to be tackled in this context [77].

7. **Crypto wallets.** Cryptocurrency wallets can be set up and controlled by smart contracts. In Islamic finance there is a large percentage of Muslims not utilizing banking services on account of ethical reasons and this population can greatly benefit by the creation of customized cryptocurrency wallets adhering to the Shariah.

8. **Supply chain finance.** [85]. The halal economy can benefit greatly by utilizing blockchain for non-repudiated data sharing between the suppliers and verification of halal certificates through the blockchain [183]. The digital platform can create opportunities for investors in the Islamic finance domain to invest in the halal supply chain.

9. **Payment systems.** Islamic finance can develop their own payment systems on the blockchain [205] and make it Shariah compliant to protect users from the interest associated with the available digital payment methods.

Our goal in this chapter is to assess and to evaluate the employability of blockchains for sukuk issuance. Using our taxonomy above, this chapter thus provides insights on application development for Islamic capital markets. We seek to answer important questions for organisational, i.e. commercial adoption of blockchain applications that are developed to support sukuk issuance. Issues, such as the emerging cost factors and their magnitude, and the benefits that blockchain would embrace for this particular financial instrument are equally important. Therefore, the rest of this chapter is centered around a concrete tokenization exercise of sukuk using the Ethereum blockchain platform. The analysis of this exercise allows us to evaluate the potentials of tokenization both quantitatively (i.e. cost assessment) and qualitatively (i.e. benefits and concerns of commercialization), providing thus the answers we are seeking for.

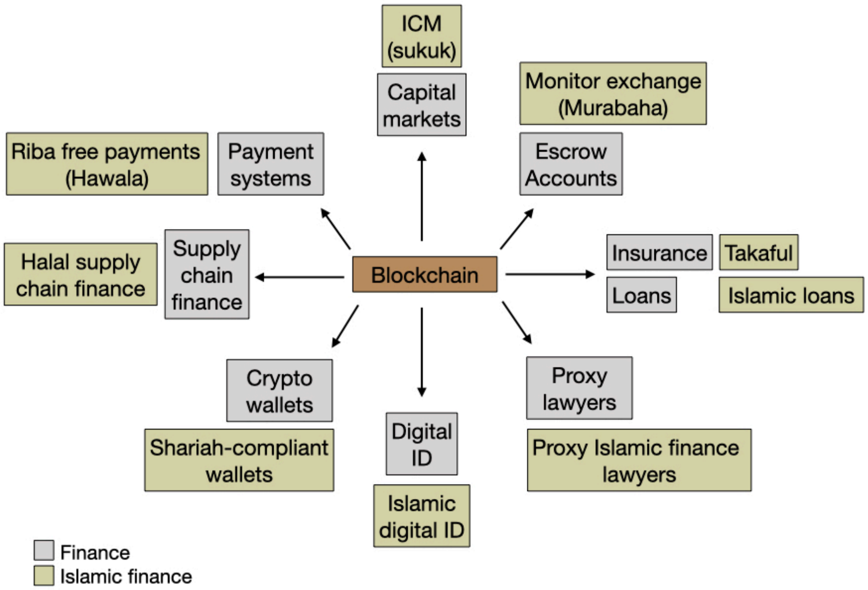


Figure 6.2: Taxonomy of Blockchain Applications in Finance and Islamic finance

6.5 Assessment of Blockchain Platforms for Tokenization

In order to assess the feasibility of sukuk tokenization by measuring its performance, related costs and addressing its benefits, it is imperative to know that sukuk tokenization relies on employing smart contracts for execution. In this section, we review the blockchain platforms available that can support smart contracts. Smart contracts are heralded as the most important application of blockchain. A smart contract is a computer program that formalizes relationships over computer networks through a combination of protocols with user interfaces [179]. They form the base of blockchain-based decentralized applications, which might function as products or services for mass usage. Smart contracts reside and are executed on the blockchain, where the correct execution is enforced by the consensus protocol. It relies on a programming language provided by the blockchain platform to encode its operations and the ways to handle user transactions. It can implement a wide range of applications including gaming, financial, notary or computation [14]. The distinguishing feature in comparison to paper-based agreements is that smart contracts are computer programs with the capability of unilaterally applying strict rules and consequences on the basis of fresh data inputs. Further the blockchain assures that everyone is seeing the same thing without the reliance on having to trust each other.

Bitcoin, the first blockchain platform to be launched, does not support complex smart contracts. There is the availability of using simple smart contracts, but their execution is costly and designing is cumbersome [48]. The main platform for implementing smart contracts is Ethereum and its high level programming language Solidity, which is Turing complete and compiled into bytecode language. A programming language is said to be Turing complete if it can computationally solve a given problem with finite resources and a programming language that is not Turing complete cannot measure up to the Turing complete programming language in terms of functionality. Each compiled smart contract is stored in the blockchain and executed by the Ethereum virtual machine (EVM) running on the network nodes. There are numerous other blockchain platforms that are providing the functionality of smart contracts and a comparison of the prominent platforms is given in Table 6.1. In case of Turing completeness, even if one programming language being used by the blockchain platform to code smart contracts is Turing complete, the table lists it as Turing complete. However, it should be verified against the programming language being used out of the available choices in that particular blockchain platform as all might not be Turing complete. A review of the listed platforms indicates that only Ethereum, NEO and Tezos have smart contracts using programming languages that are Turing complete and can serve as feasible blockchain platforms for tokenization of sukuk in case a public blockchain platform is desired for issuance. We decided to conduct a case study on Ethereum on account of the above reasons. Ripple has invested in a smart contract platform, Flare [10], which is still being tested and was therefore not in consideration for our discussion. Stellar is not a typical blockchain supporting smart contracts as it does not have a smart contract programming language or a virtual machine to support the execution of smart contract code and is hence not a part of the review process.

[10] Ajiboye, T. (2020). Ripple backs new platform for smart contracts Flare networks via its Xpring. https://www.coinspeaker.com/ripple-smart-contracts-xpring/, accessed April 17, 2020.

[11] Transaction Execution Application Language

[12] Proof of stake

[13] Unspent transaction outputs

[14] Federated Byzantine Agreement

[15] delegated Byzantine Fault Tolerance

[16] Leased Proof of Stake

Table 6.1: Comparison of Smart Contract-based Blockchain Platforms

Blockchain platform	Turing complete	Programming language	Consensus algorithm	Execution environment	Wallet Model	Public
Algorand	✗	TEAL[11]	PoS[12]	Stack	account	✓
Bitcoin	✗	Script	PoW	Stack	UTXO[13]	✓
Ethereum	✓	Solidity	PoW	EVM	account	✓
Hyperledger	✓	Go	FBA [14]	Docker	account	✗
NEO	✓	Kotlin, C++, VB.Net, F#, Java	dBFT [15]	NeoVM	UTXO, account	✓
Tezos	✓	Michelson	PoS	Michelson	account	✓
Waves	✗	Ride	LPoS [16]	Docker	account	✓
Corda	✓	Kotlin, Java	pluggable[17]	JVM [18]	UTXO	✗

6.6 Tokenization of Sukuk

The applications of smart contract technology are diverse but restricting it to the financial world, it can be conveniently said that any kind of business logic relying on data can be coded by way of smart contracts. Securities that are based on payments and rights, which are executed according to predefined rules can be coded as a smart contract in capital markets. Experiments are ongoing on the issuance of smart bonds. Sukuk issuance follows a strict Shariah law and other principles, many of which can be programmed to ensure both compliance to the Shariah and transparency for all involved increasing the mass appeal of the product amongst Muslims [19].

Sukuk al-Murabaha is a possible structure to fulfill the capital requirements of an entity, when there is an absence of an identification of a tangible asset against which investment can be sought. It is heralded as a preference when other structures using Mudarabah, Ijarah or Musharakah are not possible, since it is debt-based. Hence, Sukuk al-Murabaha cannot be traded in the secondary market as per the Shariah prohibition of not trading debt except at par value. Figure 6.3 is a diagrammatic representation of Sukuk al-Murabaha and the fundamental steps involved in the issuance process are

[17] permitting the usage of the desired consensus algorithm

[18] Java virtual machine

[19] Khan, N. (2017). Smart contracts: The future of Islamic banking. https://www.linkedin.com/pulse/smart-contracts-future-islamic-banking-nida-khan/, accessed April 20, 2020

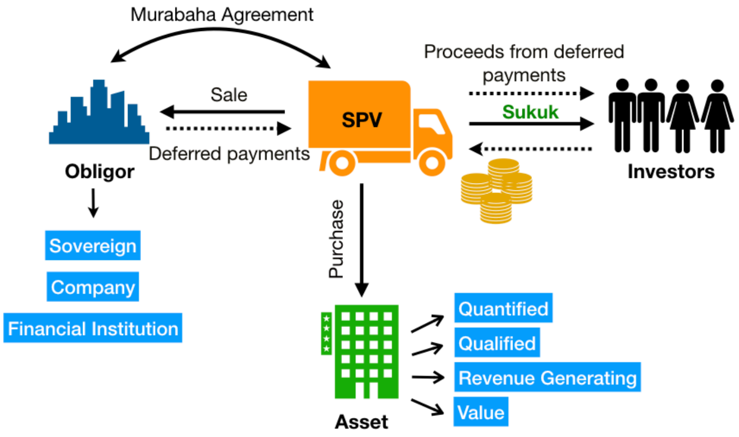


Figure 6.3: A Simplified Representation of Sukuk Al-Murabaha

given below:

- The Obligor creates a SPV to issue the sukuk. SPV is a separate legal entity with it's own assets, created by an organization to isolate financial risk, ensuring the survival of the entity even if the parent company goes bankrupt. Its role is to protect the underlying assets from investors in case of financial deficits.
- Investors agree on the sukuk and pay the principal amount to the SPV in return for sukuk certificates.
- SPV utilizes the proceeds in buying the required asset and resells the asset at a markup to the Obligor on deferred payment terms through a Murabaha contract.
- Obligor pays the installments as agreed to the SPV and the SPV transfers the requisite profit from the payment proceeds to the different investors.

An algorithm to implement the Ethereum smart contract for Sukuk al-Murabaha is given in Algorithm 1. Sukuk al-Murabaha was chosen for our consideration since our case study involved a sukuk issuance involving the Murabaha contract (refer to Section 6.7). The algorithm indicates that it is

Algorithm 1 Tokenization of Sukuk al-Murabaha on Ethereum

```
Require: Register the SPV and Obligor using their Ethereum address
Require: Initialize the payment frequency, number of sukuk coins, issue size, face value of
    the sukuk, maturity and profit rate
Require: Link to the Murabaha contract and relevant documentation is shared
Require: Register each investor using Ethereum address
Ensure: Obligor and investors buy sukuk coins to use in exchange for fiat currency.
Ensure: Obligor pays the periodic amounts for the asset
for entire period till sukuk maturity do
    if payment is due then
        pay fee to the SPV from Obligor's deferred payments and deduct the fee from the
        paid amount
    end if
end for
for entire period till sukuk maturity do
    while payment is due and number of investors $\neq 0$ do
        pay each investor the profit based on his investment
    end while
end for
```

essential to register the SPV and Obligor on the smart contract using their Ethereum address. Each investor, who intends to buy sukuk, should register through the smart contract using his Ethereum address. It is assumed that the SPV and the Obligor have entered into a Murabaha contract outside the smart contract. Notary services are not recognized online legally to the best of our knowledge and hence we excluded the purchase and sale of the sukuk asset from the smart contract. The SPV would however need to provide documentation relevant for the sukuk asset on the smart contract for the investors to see. The smart contract would collect the periodic payments from the Obligor, pay the fee to the SPV and the profit to the investors based on the payment frequency. Sukuk coins are a kind of token introduced through the smart contract.

The algorithm guided in the coding of the smart contract for Sukuk al-Murabaha [20]. The smart contract was coded in Ethereum using the programming language, Solidity. Only basic functions required for sukuk issuance were coded and necessary control statements to check for identity verification, balance requirements, conversion from fiat to cryptocurrency, event notifications, security and privacy measures were not taken into account. The purpose of the smart contract was to code a proof of concept to determine the requirements for deploying a fully functional smart contract on Ethereum in terms of cost and development effort needed. The basic functions in Sukuk al-Murabaha smart contract with the objective of their usage is given in Table 6.2. The smart contract can be deployed and run on Remix for testing purposes. Remix is a tool for writing Solidity smart contracts directly from the browser and aids in testing, debugging and deploying smart contracts [21]. Visualization of a decentralized application on the blockchain using the coded smart contract was also conducted [22].

6.7 Cost-Benefit Analysis

After introducing and analysing the technicalities related to sukuk tokenization, this section turns our analytical angle towards concerns of commercial, i.e. organizational adoption. Socio-economic,

[20] Khan, N. (2019). *sukukmurabaha1.sol*. https://github.com/nidakhanlu/Sukuk-Tokenization, accessed April 26, 2020

[21] Remix, Ethereum-IDE. (2019). Welcome to Remix documentation! https://remix-ide.readthedocs.io/en/latest/, accessed April 12, 2020

[22] OneClickDapp. (2019). BlockSukukSPV. https://oneclickdapp.com/apropos-flex/, accessed April 13, 2020

Table 6.2: Basic Functions in Sukuk al-Murabaha Smart Contract

Function	Objective
registerObligor	Registers the Ethereum address of the Obligor.
newInvestor	Registers a new investor by recording the Ethereum address, investor's name and initializing the sukuk coins owned as well as the owned sukuk as zero.
buyCoins	The registered investor buys sukuk coins.
investInSukuk	The registered investor uses sukuk coins to invest in sukuk.
enterProceeds	The Obligor pays the periodic deferred payment.
automaticPayment	The owner of the smart contract, the SPV, initiates the automatic payment for the investors from the payment proceeds collected from the Obligor.

in particular financial feasibility concerns are often bottlenecks of technology adoption, as it is also argued in [72]. Therefore, we first revisit our implementation and address its cost consequences as follows. The costs of the transactions on Ethereum were computed by deploying the Sukuk al-Murabaha smart contract on Remix and executing the various functions. The tabulation of the various costs is given in Table 6.3. The transaction fee is computed by adding both the transaction cost and execution cost in terms of the gas used. In Ethereum, gas is a unit which helps to measure the amount of computational effort required to execute a certain operation on Ethereum. The exact price of the gas is determined by the miners and the price determines the speed with which the transaction is mined and recorded on the Ethereum blockchain. The calculations in Table 6.3 were done using average gas price of 1 gwei. The Ethereum cryptocurrency can be broken into smaller denominations like *wei* similar to a fiat currency being denominated into pennies. Wei is the smallest denomination for ETH, the cryptocurrency of Ethereum. 10^9 wei is equal to 1 gwei and is used to measure gas prices [23]. The cost is computed for a single investor for automatic payment of profit and thereafter for 5 investors and it is seen that the cost is simply 5 times the cost for a single investor. Reading data from Ethereum does not cost any gas unless it is through another contract, whereas writing to the blockchain incurs a cost and hence only the functions that involve a transaction fee have been listed in Table 6.3. It is also assumed

[23] ETH Gas Station. (2019). Tx Calculator. `https://ethgasstation.info/calculatorTxV.php`, accessed April 22, 2020.

that the total number of sukuk issued have been declared before contract deployment. However, the number can be changed and a function can be provided in the smart contract to increase the number of sukuk issued in case of over-subscription. Similarly a function to destroy the smart contract after maturity or at the will of the owner of the smart contract can be provided to prevent damage in case some error is discovered in the code after smart contract deployment. The costs have been calculated using the basic functions and should only be used for a theoretical assessment of cost-benefit analysis. Costs for the practical deployment of the full smart contract might vary, including the exchange rates causing a change in the transaction fee. The exchange rate utilized corresponds to 28th December, 2019.

Table 6.3: Transaction Costs on Ethereum

Transaction (Tx)	Gas Used	Tx fee (ETH)	Costs ($)
Deploy Smart Contract on Ethereum	2737722	0.0027377	0.35043
registerObligor	63336	0.0000633	0.0081
newInvestor	278484	0.0002785	0.03565
buyCoins	406430	0.0004064	0.05202
investInSukuk	389826	0.0003898	0.04989
enterProceeds	77130	0.0000771	0.00987
automaticPayment (1 investor)	371594	0.0003716	0.04756
automaticPayment (5 investors)	1650610	0.0016506	0.21128

We compare the cost of sukuk issuance the conventional way to a blockchain-based issuance. In blockchain, the issue price and profit per annum will not affect the transaction costs but the payment frequency, the number of investors and the number of sukuk issued will directly impact the cost incurred by the issuing organization. We use the data for the transaction fee from Table 6.3 and use the sukuk issued by Aldar as a reference [93]. The details of the sukuk issuance are given below:

- Amount: $500,000,000
- SPV/ Issuer: Aldar Sukuk
- Obligor: Aldar Investment Properties

- Minimum settlement amount: $200,000
- Par amount, integral multiple: $1,000
- Issue date: 10/01/2018
- Maturity date: 09/29/2025
- Coupon frequency: Semiannual
- Issue price (% of face value): 99.718%
- Profit per annum: 4.75%
- Sukuk type: Hybrid involving Wakala and Murabaha

In order to compensate for the Wakala structure in our smart contract, we paid a fee to the SPV acting as a *wakeel* over the underlying assets. We did the following assumptions for the cost benefit analysis:

- Each investor bought the minimum number of sukuk defined in the prospectus of Aldar Sukuk.
- The Obligor, Aldar Investment Properties, also makes the periodic payment for the Murabaha contract semiannually.
- The sukuk tenor is 7 years, which would involve 14 transactions for the periodic payments by the Obligor and also profit accrued to the investors with regards to the coupon frequency.

We did the following calculations to do the cost-benefit analysis for tokenization of sukuk on Ethereum:

$$\begin{aligned} \text{\# Investors} &= \text{Amount/Minimum settlement amount} \\ &=> 500000000/200000 = 2500 \end{aligned} \tag{6.1}$$

$$\begin{aligned} \text{\# sukuk each investor bought} &= \text{Minimum settlement amount/Par amount} \\ &=> 200000/1000 = 200 \end{aligned} \tag{6.2}$$

Thereafter, we compute the total transaction costs referring to the transaction fees given in Table 6.3 for the basic functions as given below:

- ***registerObligor*** = $1 * 0.0081$ = \$0.0081
- ***newInvestor*** = $2500 * 0.03565$ = \$89.125
- ***buyCoins*** = $2500 * 0.05202$ = \$130.05
- ***investInSukuk*** = $2500 * 0.04989$ = \$124.725
- ***enterProceeds*** = $14 * 0.00987$ = \$0.13818
- ***automaticPayment*** = $14 * 2500 * 0.04756$ = \$1664.6

We chose the case of Aldar Sukuk for our study because it is an average size issuance. The usual range of corporate sukuk issuance is between \$100M to \$2B [92]. As per the financial statement of Aldar for 2019 (page 69 of [5]) the total issuance cost of the mentioned bond was \$7,165,532 or 1.43% from the total proceeds. Table 6.4 gives the cost components for tokenization on public Ethereum blockchain for a sukuk analogous to Aldar sukuk issuance. In Table 6.4 expenses mentioned refer to World Bank estimations for similar size and maturity bonds. The demarcation of the expenses was not given for Aldar and hence, we used the estimations from the World Bank for bond issuance [153]. According to an academician, the standard Shariah advisory fee is generally about one-quarter to one-half of a percent of the total value [167]. In the absence of availability of the Shariah advisory fee paid by Aldar, we consider it one-quarter of a percent to the total value.

Table 6.5 gives the cost components for tokenization of sukuk on a private/ consortium blockchain. The private blockchain and the consortium blockchain would be analogous in their cost components with the difference being in the number of nodes or computing devices employed as validators and distribution of profit accrued from the blockchain platform. In case of a consortium blockchain, the transactions for the distribution of the fee for the provided services as *wakeel* would be directly

Table 6.4: Cost Components for Sukuk Tokenization on Public Ethereum

Sukuk Component	In quoted format	USD proceeds
Issuance	99.718%	$498,590,000
Smart contract deployment		$0.35
Fees: newInvestor & buyCoins		$102,130
Fee: investInSukuk		$124,725
Fee: enterProceeds		$0.14
Fee: automaticPayment		$16,646
Fee: registerObligor		$0.01
Independent advisor	0.020%	$99,718
Legal expenses	0.030%	$149,577
Bond rating	0.100%	$498,590
Rating costs	0.005%	$24,929.50
Shariah advisory fee	0.25%	$1,250,000
Total fees and expenses to be paid upfront	0.45%	$2,266,316
Total Proceeds to Obligor		$496,323,684
All-in price (proceeds/amount)	99.26%	

proportional to the number of partners whereas it would be a single transaction in case of a private blockchain. It is assumed that the partners in setting up this private/ consortium blockchain would not be charging any fee for the transactions through their hosted blockchain and hence the transactions are all free and cost $0. We give a common Table 6.5 for the cost components of a private and a consortium blockchain highlighting the difference in the costs. We assume that the total number of nodes in the blockchain platform is equivalent to the number of partners in a consortium blockchain platform. The consortium consists of 3 partners based in Paris, Dubai and Malaysia. The private blockchain can be assumed to have 3 nodes located in Paris, Dubai and Malaysia.

The private/ consortium blockchain uses Amazon Elastic Compute Cloud (Amazon EC2) to avail a secure and resizable compute capacity in the cloud [24] for hosting the nodes. The infrastructure costs for t3.large reserved instances in EC2 will be as follows [25]:

[24] AWS. (2019). EC2 Instance Pricing - Amazon Web Services (AWS). https://aws.amazon.com/ec2/pricing/on-demand/, accessed December 21, 2019.

[25] AWS. (2019). Amazon EC2 Reserved Instances Pricing. https://aws.amazon.com/ec2/pricing/r

Table 6.5: Cost Components for Sukuk Tokenization on Private/ Consortium Ethereum

Sukuk Component	**In quoted format**	**USD proceeds**
Issuance	99.718%	$498,590,000
Smart contract deployment		$0
Fees: newInvestor & buyCoins		$0
Fee: investInSukuk		$0
Fee: enterProceeds (private Ethereum)		$0
Fee: enterProceeds (consortium Ethereum)		$0
Fee: automaticPayment		$0
Fee: registerObligor		$0
Website Hosting		$2,737
Blockchain Node Paris		$2,737
Blockchain Node Dubai		$2,856
Blockchain Node Malaysia		$2,589
Independent advisor	0.020%	$99,718
Legal expenses	0.030%	$149,577
Bond rating	0.100%	$498,590
Rating costs	0.005%	$24,930
Shariah advisory fee	0.25%	$1,250,000
Total fees and expenses to be paid upfront	0.41%	$2,033,734
Total Proceeds to Obligor		$496,556,267
All-in price (proceeds/amount)	99.31%	

Table 6.6: Cost Comparison for Sukuk Issuance vs Tokenization

Sukuk Issuance Type	Total Cost= Fees and Expenses paid upfront + Issue price
Conventional Issuance	$7,165,532
Tokenization on Public Ethereum	$3,676,316
Tokenization on Consortium Blockchain	$3,443,734

- EU (Paris) region for the blockchain node in Paris:
  1. Standard 3-Year Term: All upfront = $1096
  2. Standard 1-Year Term: All upfront = $545
- Middle East (Bahrain) region for the blockchain node in Dubai:
  1. Standard 3-Year Term: All upfront = $1154
  2. Standard 1-Year Term: All upfront = $548
- Asia Pacific (Singapore) region for hosting the node in Malaysia:
  1. Standard 3-Year Term: All upfront = $1023
  2. Standard 1-Year Term: All upfront = $543
- Website Hosting from Paris: Price is similar to the hosting of blockchain node in Paris

The other cost assumptions remain the same in the cost-benefit analysis as they were in the case with sukuk tokenization on the public blockchain. The computed results for the cost-benefit analysis are given in Table 6.6.

6.8 Sukuk Tokenization: Feasibility Analysis

The results of the performed cost-benefit analysis thus brings us closer to understand the commercial, i.e. financial consequences of sukuk tokenization. Combined with the findings of the concrete

`eserved-instances/pricing/`, accessed December 15, 2019 implementation exercise of a basic smart contract for tokenization, we articulated and assessed important feasibility concerns from the commercial, i.e. the financial market point of view, including implications for regulatory compliance. In the following, we report our findings and emphasize their significance:

1. **Issuance vs Tokenization cost comparison.** The cost incurred by Aldar for issuance was $7,165,532, while tokenization of a similar sukuk on public Ethereum involved a cost of $3,676,316. Private/ consortium blockchain recorded the minimal cost incurred for tokenization with a value of $3,443,734. The cost ratio of conventional sukuk issuance to tokenization on public Ethereum is 1.95 whereas the cost ratio of conventional issuance to tokenization on private/ consortium Ethereum is 2.10 indicating a significant reduction in expenses using Ethereum for tokenization.

2. **Role of Shariah advisors.** The role of the Shariah scholars will be paramount in tokenization and a common understanding of the programmed smart contract between the Shariah scholars, sukuk issuing organization and the technology team needs to exist to avoid potential incorrect Shariah adherence in tokenization to be legitimated as Shariah-compliant. The achievement of a common understanding is crucial for transparency and is a difficult process as it involves experts from three diverse domains to agree on a common outcome. This goal might entail the requirement of additional experts well versed in the Shariah law and technology, thus adding on to the costs. Industry exchanges on the subject give a comparatively lower Shariah advisory fee than we used but is undocumented preventing it's incorporation in our analysis. A higher limit, where the Shariah advisory fee is indicated to be in millions of dollars, also exists[26].

3. **Clearing and Settlement.** Clearing and settlement processes are more efficient by using blockchain, which ensures an automated delivery and payment mechanism in the absence of a central authority. This confines the settlement risk exposure significantly [37].

[26] SPEAR'S. (2012).Islamic finance's 'Scholar Problem': Why are Shariah scholars paid so much? https://www.spearswms.com/islamic-finances-scholar-problem-why-are-shariah-scholars-paid-so-much/, accessed March 30, 2020.

4. **Counterparty Risk.** The counterparty risk is mitigated as the settlement is occurring in real time as a result of the automation of periodic payments.

5. **Smart contract evaluation.** The smart contract coded was with minimal functions to implement a Murabaha contract for sukuk issuance. A complete smart contract would involve more functions and events, that indicate to the owner of the smart contract when a stipulated action has happened in the smart contract like the payment by the Obligor. Thus the smart contract development and deployment on Ethereum would incur higher fees.

6. **Additional Costs.** The front-end development of the smart contract into a functional decentralized application would need to be accomplished and a payment gateway would need to be used to convert the fiat currency to ETH and buying of sukuk coins if the structure involves their usage. All this would increase the costs more.

7. **Know Your Customer (KYC).** KYC is a strict regulatory measure to assure institutional compliance regarding client verification, validation and transaction monitoring. Therefore, including digitalized tools to perform KYC related to sukuk tokenization is an essential part for investor validation. There exist numerous third-party solutions for KYC compliance. Alternatively, a tool needs to be developed in-house by the issuing organization. The detailed cost assessment of KYC clearance is out of the scope of this chapter, nevertheless, raising awareness on this cost element is of high importance.

8. **Legal Issues.** Smart contracts are not considered to be legal in most jurisdictions and as such a legal contract would still need to be drawn up for the investors for their entitlement to a share in the underlying asset.

9. **Absence of an online notary.** The implemented smart contract focuses only on sukuk issuance to the investors whereas the Murabaha sale and purchase is conducted outside the blockchain network. This is primarily because the mechanism of online notary is not available in most jurisdictions as of now, to the best of our knowledge.

10. **Data privacy.** Privacy issues would need to be tackled when using blockchain and if available for this kind of a structure, privacy-preserving blockchain platforms should be employed. An alternative strategy would be to go for a hybrid of a traditional database for private data interoperable with a blockchain platform for recording transactions. The development skills needed to achieve either of the two is not easily available, thus adding on to the development costs.

11. **Scalability and throughput.** Blockchain is still in the early stages of development with scalability and performance bottlenecks impeding its mass scale usage [53, 31].

12. **Key management.** Management of public-private key pairs associated with an Ethereum address and a more than basic technical awareness from the user is expected to engage with the blockchain platform.

13. **Vulnerabilities in smart contracts.** Post deployment on Ethereum, the smart contract cannot be updated to remove any potential coding errors and any undetected errors have the potential to be exploited like the DAO attack in which an anonymous hacker stole over $50M worth of ETH [131]. Efforts should be made to adhere to a secure development process for smart contracts on the blockchain and deploy them post an optimum security analysis [81], otherwise their usage in tokenization can make them vulnerable to attacks causing major losses [132].

The above analysis indicates that to ensure economic viability for tokenization of sukuk, the technology needs to be developed to a level where it can be aptly used in the market on a large scale and appropriate regulations have been framed by governments for recognition of an online notary. Additionally there should exist legalization of smart contracts in all the concerned jurisdictions to ensure dispute resolution and complaints redressal. It is recommended for organizations embarking on the initiative to conduct a cost-benefit analysis adding the costs listed above to the assessment conducted in this to come to a more just estimate of the process.

6.9 Conclusion

In this chapter we evaluated the present challenges in sukuk issuance and discussed circumvention of some of them using blockchain. We discussed the blockchain platforms, in the light of their architecture, that can prove to be suitable for sukuk tokenization. We elaborated on a taxonomy for blockchain applications in finance and the Islamic finance domain in particular. We conducted a case study on tokenization of Sukuk al-Murabaha on Ethereum and coded a basic smart contract to gauge the contract development complexity and effort required. Developers with the requisite skills are not readily available and Islamic finance personnel should be trained to cater to this need in the sector. Our performed cost-benefit analysis of sukuk tokenization indicates that tokenization itself, leveraging on blockchain, incurs significantly less expenses when compared to conventional sukuk issuance. Furthermore, our more detailed analysis shows that sukuk issuance on the public Ethereum blockchain incurs a higher cost than tokenization on a private/ consortium Ethereum blockchain platform. The results are, however, dependent on the concrete implementation characteristics and assumptions based on the particular application domain, such as the choice of the number of nodes, sukuk tenor, number of investors and other similar factors. Feasibility analysis of sukuk tokenization on Ethereum needs to be considered in the light of economic viability, when viewed from the broader perspective considered in Section 6.8, and the advantages it offers in terms of expanding the investor base and proving to be a solution for the funding needs of SMEs.

As an important contribution, this chapter provides a step-wise, systematic approach to assess and to analyse fundamental elements of commercial feasibility of sukuk tokenization. By addressing the fundamental factors of cost-benefit analysis in Section 6.7, such as the cost factors of blockchain transactions, and by conceptualising the main findings and concerns of adoption in Section 6.8, we provide a solid assessment framework for organizations that intend to tokenize sukuk. However, it is crucial that the investors ensure that appropriate regulations are in place for sukuk tokenization to protect their interests before investing in blockchain-based sukuk. Technology is developing at a rapid pace and eventually regulations will follow to discipline its usage. Besides, technological advancements would result in more cost reductions in their employment with the passage of time. Therefore, hybrid arrangements which take into account the existing regulations and legacy systems should be integrated with blockchain to develop novel structuring methodologies for sukuk tokenization to leverage on the benefits of the technology.

The problems we have today, cannot be solved by thinking the way we thought when we created them.

Albert Einstein

7

Decentralized Donation Application for a Crowdfunding Platform

Donation is a tool that can be coupled with crowdfunding for social impact but remains plagued by many inherent shortcomings. This chapter introduces a novel model in the form of a decentralized app developed and deployed on the Ethereum blockchain. The decentralized app solves the challenges present and optimizes the process of donation in a specific obligation of Muslims, namely Zakaah. Load and stress tests on the prototype of the smart contract in the public testnet of Ethereum were analyzed to gauge the feasibility of mass usage. Similar tests were done in Hyperledger to conclude on the optimum blockchain platform for donation. A novel strategy was proposed to enhance the throughput of Ethereum. The testing is a pioneer in evaluating the throughput and feasibility of a blockchain-based financial product and provides a benchmark to validate the business and technical hypotheses of other similar financial products and services.

7.1 Introduction

The most comprehensive reports state that the world housed 736 million people, which was approximately 10% of the world's population in 2015, below the International Poverty Line with the poverty-ridden population surviving on less than $1.90 a day [180]. Zakaah is an obligation on Muslims to donate 2.5% of their accumulated wealth annually for charitable causes. $1.25 million donated by Zakaah helped 8.3 million people in 2015 [94]. The process of donation is ridden with several problems. There exists reliance on third parties for donation-based payments [64], absence of an easy and transparent way to donate and an inefficient distribution of money depriving the one's in need. The charities presently are always under scrutiny for the discharge of money made available to them while the end receivers remain at the mercy of charities. There are presently 1.7 billion Muslims with no transparent service to aid in the discharge of the religious obligation of Zakaah.

The enumerated problems and the compelling need for a transparent donation system motivated the development of the Ethereum decentralized app, Zakaah dapp, that forms the foundation of this chapter. The dapp is designed to protect against third party fraud, ensure auditable transactions and execute real-time donations directly to the receivers. A smart contract was coded to optimize the zakaah collection, distribution and impact documentation process through the dapp. Blockchain is a nascent technology and there does not exist another similar usage of smart contracts that could have aided in the design and development process. Zakaah dapp is a pioneer in this respect.

The chapter is organized to give the relevant background in Section 7.2. The functional architecture of the Zakaah dapp is discussed in Section 7.3. Section 7.4 of the chapter highlights an anomaly detected during the testing of dapp on the public testnet of Ethereum and exploits the anomaly to analyze submission of transactions and mining times independently. Zakaah is mostly discharged in the month of Ramadhan, when fasting is observed by Muslims. Therefore the application has to be resilient to the extra load during this month. In Section 7.5, the chapter elaborates the test results of three different strategies employed to measure the throughput of Ethereum during periods of extra load on the dapp and discusses the feasibility of the different approaches adopted. The chapter also depicts the test results of servicing the requests of multiple users through a single node functioning as an Ethereum client in comparison with setting up a single dedicated node per user.

An analysis of the private networks of different blockchains has already been conducted [53]. Therefore a comparison of stress test results on the public Ethereum testnet network and the private Hyperledger development environment was dealt with to aid in the proposition of an optimum scalable blockchain-based solution to the problem. Related work is highlighted in Section 7.6. Conclusions drawn and future work is discussed in Section 7.7 together with the proposition of a novel strategy to improve the throughput of Ethereum and increase the probability of transaction inclusion in the blockchain. The decision was reached as a conclusion of the tests conducted, which spans 0.3 million transactions successfully submitted on the public Ethereum testnet, Ropsten over a duration of 57 days and includes 3 contract creations on the blockchain.

7.2 Background

There are certain Shariah requirements which need to be adhered to while giving zakaah and our proposition, Zakaah dapp, intends to automate the accomplishing of these Shariah guidelines through smart contracts. Shariah refers to the Islamic laws that govern both the religious duties and the life of a Muslim. The guidelines that need to be taken care of during zakaah distribution and collection are as follows:

1. The zakaah obligation is the responsibility of the donor and is best discharged by the donor himself to the end receiver as per his own understanding.

2. It should be given in the land where the wealth is unless there is a specific need to send it elsewhere to people, who are more in need, in another country or poor relatives.

3. Zakaah has to be given according to the eight categories defined in the Shariah.

4. It is permissible to give zakaah to someone one trusts to discharge it on our behalf as per the Shariah categories.

5. If the zakaah money is given to a charitable organization and they lose it, then the obligation of the donor is not fulfilled. Either the charitable organization has to forfeit the loss to pay

zakaah or the donor has to give zakaah again. The same would be the case if the designated charity does not distribute the zakaah at all due to fraud or distributes it in a way that is not Shariah-compliant.

7.2.1 Problems in Donation

The advent of migration and international job relocation has brought up new challenges in discharging the obligation of zakaah. The people settled away from their homeland are not aware of their new environment and mostly the western societies are comparatively affluent so finding the right person to give your Zakaah to, has become a significant issue. Many people desire to give their Zakaah to people in their own homeland, as they are more aware of the poor population there. This led to the mushrooming of *Zakaah Organizations* throughout the world, which collected money on behalf of the donors to distribute it amongst the eligible. As with all charitable organizations, zakaah platforms faced the same issues of manhandling of resources, donors dissatisfied with the lack of transparency in zakaah distribution and possible fraud in the channel between the organization and the end receiver of zakaah. The problems can be summarized as follows:

1. Reliance on third parties for payment.
2. Absence of an easy way to give money.
3. Inefficient distribution depriving the one's in need.
4. Compelling need for transparency.
5. Targeted donation to realize the goals as per Shariah guidelines.
6. Adherence to Anti-Money Laundering (AML)/ Counter Terrorist Financing (CFT) guidelines.
7. Prospective payers are not recognized or encouraged to pay.
8. Long-term vision for capacity building is missing.

7.2.2 Circumvention using Blockchain Technology

Blockchain can aid in making the collection, distribution and recording the impact of zakaah easy and efficient. Some of the ways it can help are as follows:

1. Blockchain absolves the need for intermediaries and hence discharging zakaah using a blockchain-based application will remove the reliance on intermediaries.

2. Blockchain can be coupled with Artificial Intelligence to determine priority for recipient categories and make it visible to the donors so the donations are accorded accordingly.

3. Blockchain increases the transparency in donations.

4. Blockchain can be used to categorize the recipients and hence make it feasible for the donors to make targeted donations to realize certain goals like crowdfunding a Shariah-compliant project.

5. The impact of the zakaah can be recorded on the blockchain to encourage the population, who fall in eligibility criterion for zakaah but do not donate, to participate in the humanitarian activity.

A dapp is a decentralized app that enables users to interact through a HTML/JavaScript web application using a JavaScript API with the blockchain. An Ethereum dapp has its own business logic encoded in a smart contract or several smart contacts deployed in Ethereum to ensure persistent storage of data and transactions.

7.3 Functional Architecture

Zakaah dapp is conceptualized to fulfill the obligation of zakaah according to a subset of categories defined in the Shariah and aid in achieving some of the Sustainable Development Goals of United Nations Development Programme (UNDP). A charitable endowment, **waqf** [156] is responsible for reviewing the verification of the authenticity of the projects before exchanging the Ethereum token, Zakaah Coins, into physical currency. The verification of the projects hosted on the Zakaah dapp is done by charities, where the addition of the latter is done by the waqf. The entire architecture is built on donors and receivers as the primary agents. Charities function solely as authorizing entities and waqf is the body that triggers the exchange into physical currency for the digital currency.

The donors and charities register through the smart contract. A donor on registration can see a list of all the projects with their respective charities, funding goal and category. The donor purchases Zakaah Coins by transferring fiat money to the bank account of the waqf. The exchange rate and the third party payment integration in the dapp to facilitate the bank transfer is to be determined by the business venture using the dapp. When the donor has Zakaah Coins in his wallet, he can donate these coins to any project he deems fit. Once the funding goal of a project is reached, the project can request the charity for exchange of coins into physical currency.

Charities will evaluate the impact of the project. For example if a project wants to build a well for providing drinking water then they would have to upload on the blockchain the government permission to utilize that property for the said purpose. This can be done through a function provided in the smart contract. It is envisaged that images of receipts, documents and the like will be uploaded on platforms like dropbox and the link shared on the dapp. All the donations and all other data are publicly available. The identity of the donors is private and can be seen only by the donor himself and the waqf. The smart contract ABI of the prototype of this dapp, which is deployed in the Ethereum testnet, Ropsten [1] can be accessed together with the deployed address from a github repository [2], facilitating public usage of the smart contract for testing purposes. Fig.7.1 depicts the functional architecture of the dapp. The design goals were accomplished keeping in mind the need for transparency, auditability and security.

7.4 Anomaly Detection in Dapp Testing

The implementation of the smart contract was done by using Truffle [3] with Webpack [4]. A live demo of the main functions of the smart contract in the testnet environment *ethereumjs-testrpc* was

[1] Ropsten Revival Testnet, https://ropsten.etherscan.io/

[2] Blockchain Stress Testing Scripts and Results, https://github.com/nidakhanlu/blockchain-stresstests

[3] Truffle development framework, http://truffleframework.com/

[4] Webpack module bundler, https://webpack.js.org/

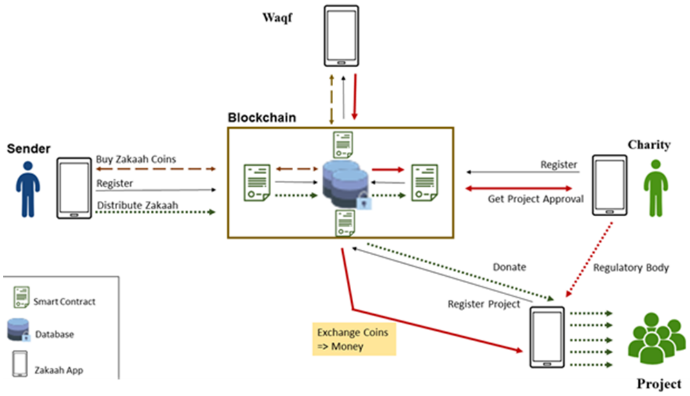
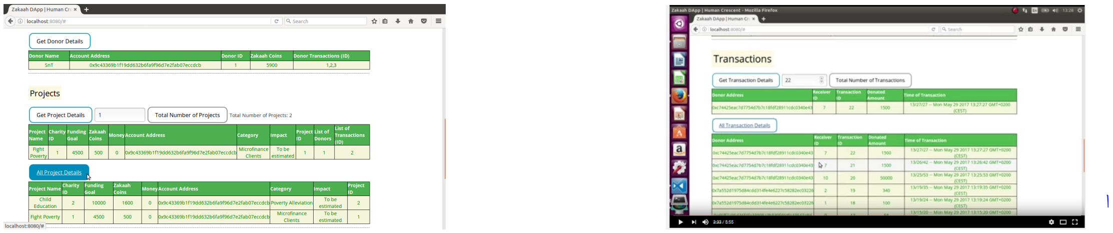


Figure 7.1: Functional Architecture of the Zakaah Dapp



Get Donor Details

Donor Name	Account Address	Donor ID	Zakaah Coins	Donor Transactions (ID)
SnT	0x9c43369b1f19dd632b6fa9f96d7e2fab07eccdcb	1	5900	1,2,3

Projects

Get Project Details 1 Total Number of Projects Total Number of Projects: 2

Project Name	Charity ID	Funding Goal	Zakaah Coins	Money	Account Address	Category	Impact	Project ID	List of Donors	List of Transactions (ID)
Fight Poverty	1	4500	500	0	0x9c43369b1f19dd632b6fa9f96d7e2fab07eccdcb	Microfinance Clients	To be estimated	1	1	2

All Project Details

Project Name	Charity ID	Funding Goal	Zakaah Coins	Money	Account Address	Category	Impact	Project ID
Child Education	2	10000	1600	0	0x9c43369b1f19dd632b6fa9f96d7e2fab07eccdcb	Poverty Alleviation	To be estimated	2
Fight Poverty	1	4500	500	0	0x9c43369b1f19dd632b6fa9f96d7e2fab07eccdcb	Microfinance Clients	To be estimated	1

Transactions

Get Transaction Details 22 Total Number of Transactions

Donor Address	Receiver ID	Transaction ID	Donated Amount	Time of Transaction
0xc74425eac7d7754d7b7c18fdf28911cdc0340e43	7	22	1500	13/27/27 -- Mon May 29 2017 13:27:27 GMT+0200 (CEST)

All Transaction Details

Donor Address	Receiver ID	Transaction ID	Donated Amount	Time of Transaction
0xc74425eac7d7754d7b7c18fdf28911cdc0340e43	7	22	1500	13/27/27 -- Mon May 29 2017 13:27:27 GMT+0200 (CEST)
0xc74425eac7d7754d7b7c18fdf28911cdc0340e43	7	21	1500	13/26/42 -- Mon May 29 2017 13:26:42 GMT+0200 (CEST)
0xc74425eac7d7754d7b7c18fdf28911cdc0340e43	10	20	50000	13/25/53 -- Mon May 29 2017 13:25:53 GMT+0200 (CEST)
0x7a552d1975d84cdd314fe4e6227c58282ec03226	2	19	340	13/19/35 -- Mon May 29 2017 13:19:35 GMT+0200 (CEST)
0x7a552d1975d84cdd314fe4e6227c58282ec03226	1	18	100	13/19/24 -- Mon May 29 2017 13:19:24 GMT+0200 (CEST)
[illegible]	[illegible]	[illegible]	[illegible]	13/15/20 -- Mon May 29 2017 13:15:20 GMT+0200

Figure 7.2: Screenshots of Zakaah Dapp

accomplished [5]. Testnets simulate the Ethereum network and EVM (Ethereum Virtual Machine). *ethereumjs-testrpc* is a local testnet used for early stage testing in Ethereum. After the development and testing of the dapp on *ethereumjs-testrpc*, testing on the Ethereum public testnet, Ropsten, was accomplished. In order to connect to Ropsten, Geth [6] is used, which is useful for connecting to public networked testnets. Connecting to Ropsten through Geth simulates the real Ethereum network. This testing was done through one node connected to a wireless network and the other to an Ethernet wired connection to simulate the behavior of both kinds of users. The behavior of the dapp was studied in case of no Internet connectivity. It is a good design practice to test the behavior of any application when Internet connection fails. When Internet connectivity is non-existent or fails intermittently a user might press "Enter" multiple times when he sees nothing is happening [7]. It is essential to ensure the response of the application for this kind of user behavior.

Everything that Geth persists is written inside it's data directory stored on the local node [8]. It was observed that any transaction that is submitted in the absence of network connectivity gets stored in the local node's data directory for Geth and is broadcasted to the transaction pool when network connection is restored. Transactions in the dapp are being submitted using *web3.eth.sendTransaction* [9] and not *web3.eth.sendRawTransaction*. The latter is used for broadcasting transactions signed offline. Essentially both the signing of the transactions and their submission with the return of the hash of the transaction is being done in the absence of network connectivity. This anomaly is demonstrated in a video, which was recorded during testing [10]. Transactions were submitted with no Internet connectivity through the Zakaah dapp and through a bash script programmed to simulate the user in

[5] Demo of the Zakaah Dapp, https://www.youtube.com/watch?v=Bh3Pkg_UU0k

[6] Geth: go-ethereum, https://github.com/ethereum/go-ethereum/wiki/geth

[7] Zeichick, A. (2017). Designing always-on apps that don't crash when the Internet connection fails. In *Hewlett Packard Enterprise*. https://www.hpe.com/us/en/insights/articles/how-to-design-software-that-doesnt-crash-when-the-internet-connection-fails-1705.html, accessed November 2017.

[8] Ethereum: Backup and Restore, https://github.com/ethereum/go-ethereum/wiki/Backup-&-restore

[9] JavaScript API, https://github.com/ethereum/wiki/wiki/JavaScript-API#web3ethsendtransaction

[10] Video depicting offline submission of transactions, https://www.youtube.com/watch?v=oHVCQvaUbxo

submitting transactions through the prototype to Ropsten.

7.5 Load and Stress Testing

Zakaah is an obligation which is discharged majorly during the month of fasting, Ramadhan. Any application targeting zakaah donors should be able to handle the increase in load during this time. It was therefore essential to do stress tests on the Ethereum blockchain through the Zakaah smart contract. A prototype of the smart contract was used to do stress testing on the testnet, Ropsten. The prototypes of the smart contract (Ethereum) and chaincode (Hyperledger), the scripts used and the test results can be accessed through the github repository [11]. The tests on Ropsten were conducted through 11 accounts. The tests were run on two virtual machines, a Windows-based operating system and another on Proxmox Virtual Environment [12]. Geth version 1.6.7-stable [13] linux-amd64 and Go version 1.8.1 [14] were used for the tests. The prototype of the Zakaah smart contract was deployed on Ropsten. All transaction hashes and timestamps can be verified through Ropsten. The gas price used in the transactions varies linearly between **30** Gwei and **31** Gwei and has a **Transfer Wait** of **0.5 minutes** and a transaction **Confirmation Time** of less than **1 second** [15]. The stress tests on Hyperledger were done on Fabric v 0.6 [16]. Vagrant development environment was used with security and privacy disabled. A single node private network was used to complement the already available higher limit of the throughput, 3000 transactions per second [17] of a single node Ethereum private network in Parity [18].

[11] See 2

[12] Proxmox virtual environment, https://www.proxmox.com/en/

[13] See 6

[14] The Go programming language, https://golang.org/

[15] ETH Gas Station: http://ethgasstation.info/

[16] Writing, building and running chaincode in a development environment, http://fabricdocs.readthedocs.io/en/origin-v0.6/Setup/Chaincode-setup.html

[17] Internal testing for Parity-only network, https://blog.ethcore.io/onwards/

[18] Parity, Ethereum browser, https://parity.io/

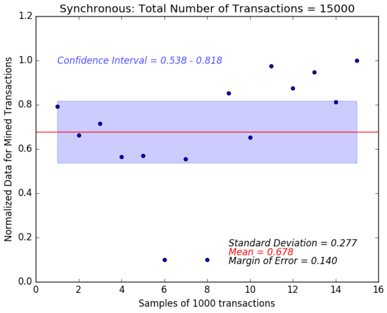


Figure 7.3: Synchronous:σ=0.277, μ=0.678

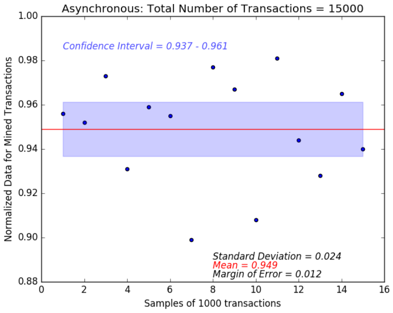


Figure 7.4: Asynchronous:σ=0.024, μ=0.949

7.5.1 Throughput Comparison of Synchronous, Asynchronous and Offline Submission of Transactions

Transactions in counts of 10, 100, 1000 and 10000 were submitted on Ropsten through the deployed smart contract through a single account per node. It was observed that not all transactions were mined even after a period of 24 hours. Three different mechanisms were used to submit transactions. After conducting multiple tests with a single account, 10 accounts were created to submit transactions in parallel through a single node to study the servicing of requests by a node functioning as an Ethereum client connected to the blockchain. Tests with 10 accounts were repeated to get an adequate number of samples consisting of a large number of transactions (15000 and 40000) to calculate the standard deviation, margin of error, mean and confidence interval with 95% confidence level on normalized data for successfully mined transactions to reach an unbiased conclusion on the throughput. The value of z critical is 1.96.

Synchronous. A stream of 1000 transactions was submitted to the blockchain. The test was repeated 15 times and the results can be seen in Fig.7.3. The shaded region represents the confidence interval 0.538 - 0.818, σ is 0.277, μ is 0.678 and margin of error is 0.140.

Asynchronous. Batches of 10 transactions were submitted after a delay of 80 seconds to the blockchain through the Ethereum client. In each test 1000 transactions were submitted and the test was repeated 15 times. The test results can be seen in Fig.7.4. The delay of 80 seconds was found to give the maximum throughput in the network conditions the tests were

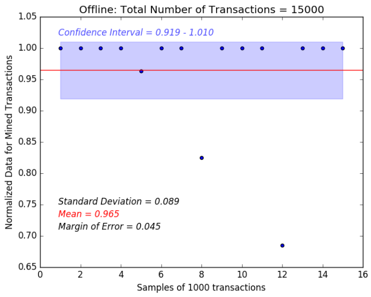


Figure 7.5: Offline:σ=0.089, μ=0.965

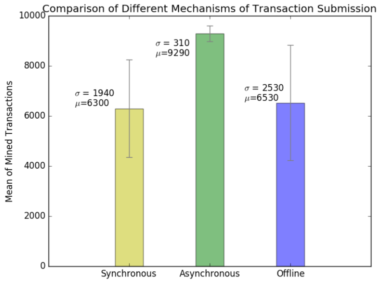


Figure 7.6: Comparison for 40000 Transactions

conducted. Other delays of 10, 12, 15, 70 seconds among others were tried but failed to give an optimum throughput. Fig.7.4 depicts that the confidence interval is smaller 0.937 - 0.961 accompanied by an increase in throughput with a μ of 0.949. The margin of error is 0.012 and σ is also much less at 0.024.

Offline. Transactions were submitted to Geth with no Internet connectivity and post network connection establishment they got broadcasted automatically to the transaction pool for mining. The results can be seen in Fig.7.5. Both the margin of error, 0.045 and σ, 0.089 are small compared to synchronous but are more when compared to asynchronous. The confidence interval also is also wider than asynchronous accompanied by a 1.6% increase in throughput as compared to asynchronous.

7.5.2 Plausible Explanation for Increase in Throughput for Asynchronous Submission

Ethereum operates in an asynchronous environment, the Internet. The command used to submit the transaction through the JavaScript Console in the dapp and Geth, *web3.eth.sendTransaction* is with a callback and this is also asynchronous in nature. Therefore an asynchronous submission of transactions gives improved throughput. If batches of data are transmitted at periodic timeouts the transactions that get mined increases by 27.1% in a small population size (see Fig.7.4) and 29.9% in a large population size (see Fig.7.6). The size of the batch and the timeout can be determined by the prevailing network conditions.

7.5.3 Summary of Testing

Offline test was conducted using 10, 1000 and 10000 transactions from a single account first. Both 10 and 1000 transactions got mined without any transactions being dropped off by Geth as per heuristics and age. However when 10000 transactions were submitted only 4598 got mined and the rest were rendered invalid. The size of the local cache was increased from 128 MB to 1024 MB and the tests were repeated with 10 accounts as mentioned before and the total number of transactions that got mined increased from 4598. However it still remains to be tested if the increase in the number of transactions mined was due to increase in the cache size of Geth on the Ethereum client or the increase in the number of slots in the transaction pool for multiple accounts (4096 transactions with 1024 in queue were the transaction pool statistics for Geth on the Ethereum client for multiple accounts with each account permitted to have 16 executable transactions and 64 transactions in queue [19]). It was also observed that during offline submission, the mined transactions were in blocks, which had more transactions than found normally in the testnet. Hence an increase in the number of transactions in a block was witnessed.

Throughput was also seen to be affected by whether the network connection to the blockchain is through wireless or an Ethernet cable. The wired Ethernet used had a download speed of 814.59 Mbit/s and an upload speed of 498.60 Mbit/s. The wireless had a download speed of 14.12 Mbit/s and an upload speed of 1.51 Mbit/s. Wireless was from a distance of 13.97 km from the best server and reported a network latency of 43.824 ms. The wired Ethernet was from a distance of 14.86 km from the best server and recorded a latency of 4.687 ms [20]. The load testing was done on both the environments whereas the stress tests to get the standard deviation were executed on the wireless in the wake of a larger number of users using the wireless to access the services on the Internet [21].

[19] Ethereum GitHub. Transaction Pool Go file, Lines 125-145, https://github.com/ethereum/go-ethereum/blob/master/core/tx_pool.go

[20] Tests conducted using https://raw.githubusercontent.com/sivel/speedtest-cli/master/speedtest.py

[21] Snow, J. (2016). NTIA survey: More Americans using wireless internet at home. https://www.fedscoop.com/ntia-survey-more-americans-welcome-wireless-internet-into-their-home/,ac

100 synchronous transactions got mined in an Ethernet connection but the throughput decreased by a considerable percentage over a wireless connection. Asynchronous submission of transactions with the delay of 80 seconds gave a throughput in the range of 92.9% - 94.9% in both Ethernet wired and wireless connections and in all ranges of the transactions sent and came across as the most suited mechanism for submitting transactions to the Ethereum blockchain.

7.5.4 Analysis of Submission and Mining Functions

The anomaly detection during dapp testing provided the opportunity to study the submission of transactions separately from the mining. A test was conducted by sending 1000 transactions in offline mode to measure the submission and mining times separately. The test was repeated 6 times and the average time for submission was found to be 357.67 seconds and average mining time for 1000 transactions was found to be 294.67 seconds. The throughput in the case of 10000 transactions was extremely poor in offline mode and hence only one sample data was chosen which recorded a throughput of 94.9% (see the data used in 2°). The submission time for 10000 transactions was 4240 seconds whereas the mining time was 10619 seconds. It was thus observed that mining time increases at a much larger rate than submission time and is much higher than submission time when there is network congestion by a lot of pending transactions. However mining time is less or equivalent to the submission time for periods of low network traffic. It was also observed that transactions get mined within seconds after being broadcast from the Geth node. However on account of network congestion, they remain pending in Geth node and their broadcast is delayed. Therefore a larger cache size would affect the throughput but more validation by testing is needed.

7.5.5 Effect on Throughput by Serial and Parallel Submission of Transactions

The throughput of Ethereum can be increased if the number of transactions that are submitted to the blockchain increases. Ethereum has a flexible gas limit for the blocks and thereby the gas limit will

cessedNovember2017.

increase with the increase in the number of transactions as per Ethereum whitepaper [22], resulting in an increase in the throughput. A test was done by submitting 100×2 synchronous transactions in parallel from two nodes from two accounts and then submitting 200 synchronous transactions from a single node from one account over an Ethernet wired connection. There was a difference in the total time taken by serial and parallel submission in this case. When parallel submission of transactions was done from two different nodes, then the submission time was much less and there was an increase in the throughput. In parallel submission of transactions all 200 were mined and in serial submission only 143 were mined, hence there was a decrease in mining time observed in serial submission. This is also because of the limit on the transactions by a single account in the transaction pool [23]. Tests were repeated for 1000 transactions from a single account on a node and 10 accounts submitting a total of 1000 transactions in parallel from the same node. It was observed that the serial submission had an average normalized mean throughput of 0.579 as compared to 0.717 in parallel submission for 6 samples, each of 1000 transactions. This led to the conclusion that utilizing a single node for an individual user is both infeasible technically and practically.

7.5.6 Comparison with Hyperledger

The load and stress tests in Hyperledger were done on the same pattern of 10, 100, 1000 and 10000 transactions submitted in a synchronous stream. The test results show that the throughput of Hyperledger is very high compared to the public Ethereum testnet. No transactions failed in Hyperledger but a more thorough evaluation needs to be done by increasing the number of nodes in the private network to see the reduction in the transactions handled per second and come up with an appropriate number of nodes in which a reasonable throughput is obtained. A similar evaluation should be done for Ethereum private network by altering relevant parameters like block gas limit to include more transactions. Such data would help in setting up private networks in different geographical regions similar to the offices of Islamic Relief, UK that function in different countries to administer the col-

[22] Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper

[23] See 19

lection and distribution of Zakaah [24]. There is already data on comparison of private networks of Hyperledger and Ethereum [53] but no such comparison was available between the public Ethereum network and Hyperledger to complete the research on different options available. Further the cost incurred is higher in setting up a private network and in Ethereum security features are not built-in like in Hyperledger. This precludes a higher investment of capital. Tests were repeated 6 times for a batch of 1000 transactions from a single account per node and Ethereum recorded an average mining time of 605.33 seconds with Hyperledger at 300 seconds for 6000 transactions in total. The mean throughput of Ethereum was 57.95% and Hyperledger was 100%. The results (calculations and data [25]) are good for setting a base for deciding which blockchain to use but they do not do justice to the real throughput of the blockchain platforms. This is because as seen in subsection 7.5.5, the throughput of Ethereum increases with increase in the number of nodes sending transactions till it reaches a certain maximum limit [53], whereas it decreases in Hyperledger [53].

7.6 Related Work

Ethereum is amongst the most popular blockchain platforms and emerges as the leader on account of its smart contract functionality. It is thus surprising that there are rare studies, if any, having been conducted on analyzing the platform outside formal models. Gervais et al. [68] introduce a novel blockchain simulator to analyze the security and performance of proof of work blockchains like Ethereum. The present work differs in being an analysis of the performance of the Ethereum public test network, which is active and being used globally. In [9] Anderson et al. categorize the transactions in Ethereum into currency transfers and contract creations. This is different from the work accomplished in this chapter where transactions have been critically evaluated for throughput enhancement and used to perform stress tests on the blockchain. In [53] a benchmarking framework has been proposed to analyze private blockchains focusing on the performance metrics of existing blockchain platforms. Similar work has been done in Ethereum [26] for analyzing throughput of trans-

[24] Islamic Relief. (2015). Annual Report. http://www.islamic-relief.org.uk/about-us/annual-reports/, accessed November 2017.

[25] See 2

[26] See 17

actions in private network whereas benchmarking for full blockchain processing time has also been accomplished [27]. [69] negates the assumption that information dissemination in the Bitcoin blockchain network is directly received by the nodes. Attempts have been made to explain the factors resulting in the probability of transactions being mined in Ethereum as 70% [28]. The work accomplished in the present chapter comes very close by providing a transaction inclusion probability range of 63% - 67.8% with a 95% confidence level for transactions submitted synchronously (see Fig. 7.3 and Fig. 7.6). In [115] Ahmed et al. propose a decentralized smart contract system to preserve transactional privacy on the blockchain. The work in the literature so far does not embark on any analysis of a dapp and a smart contract use case. Additionally the test results in the chapter obtained are the product of submitted transactions and not simulations. This work is a pioneer in many respects including providing a validated solution to increase throughput and probability of transaction inclusion by 92.9% - 94.9%.

7.7 Conclusions and Future Work

The mechanism of asynchronous submission of transactions and the offline collection of transactions for broadcasting later on can be merged to realize a practical methodology to submit transactions in the blockchain. Asynchronous submission can be impractical depriving the users of accessing the blockchain during the timeouts. A combination as stated above of asynchronous with offline mechanism can be more realistic from the perspective of providing a good user experience for the dapp and can be seen in Fig.7.8. During the timeout for the combination methodology, the read requests by the users can still be returned by Geth searching the local copy of the blockchain. A new block is created every 15 seconds in Ethereum [29] and to ascertain it's inclusion in the main chain at least 3 block confirmations are needed [30] so a timeout of even 45 seconds would be able to fetch relevant data for the read queries by the users if they are present in the recently added blocks. The transactions submitted would get stored in the local cache for Geth.

[27] Ethereum benchmarks, https://github.com/ethereum/wiki/wiki/Benchmarks

[28] ETH Gas Station: Current dynamics of transaction inclusion on Ethereum, https://medium.com/@ethgasstation/current-dynamics-of-transaction-inclusion-on-ethereum-ae8912edc960

[29] See 28

[30] Coinbase Support: How do I send digital currency ?, https://support.coinbase.com/customer/portal/articles/971437

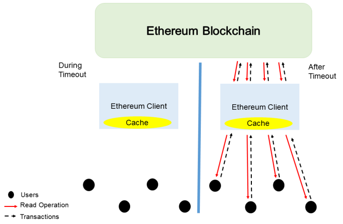


Figure 7.7: Proposition I

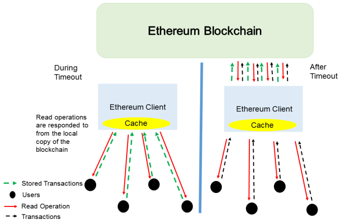


Figure 7.8: Proposition II

In the implementation governing asynchronous transaction submission, the throughput has already been evaluated and tested to lie in the interval 92.9% - 94.9% and this implementation can be visualized as in Fig.7.7. The tests for a combination of the two above mentioned mechanisms were carried out by selecting random timeouts. A timeout of 30 seconds was chosen in which there was no Internet connectivity and this was followed by a period of 30 seconds in which the node was connected to the blockchain. A bash script was run in parallel throughout the time transactions were submitted to repeat this timeout persistently. A mean throughput of 64.76% was recorded. The second test was conducted with a timeout of 10 seconds of no Internet connectivity followed by Internet connectivity for 80 seconds. A mean throughput of 53.04% was obtained. The tests were repeated for a total of 40000 transactions. It is thus observed that the choice of timeout has a major impact on the throughput.

Another peculiar observation during testing for the propositions was that the first batch of 10000 transactions had a throughput of 94.53%, which was followed by another batch with 64% and then it dropped drastically in the subsequent two batches to 25.47% and 25.83% respectively. The possible explanation for this is that blockchain is presently not able to handle a high load. The throughput will be good for low loads and fall sharply for a high load on the blockchain network. Asynchronous divides the load through the timeouts. In the wake of the improvement in throughput asynchronous transaction submission offers, it is imperative that more work be done on Proposition II (Fig.7.8) to provide a continuous access to the blockchain service, while retaining the throughput increase recorded in Proposition I (Fig.7.7).

Stress test results reveal that maximum throughput is obtained in asynchronous submission of transactions and it is the most stable in terms of performance. Scalability issues exist in both Ethereum and Hyperledger. The ideal throughput evaluation in this chapter might decrease when an extremely high number of transactions are submitted in parallel from different nodes in Ethereum on account of network congestion. In Hyperledger too the performance would deteriorate on account of increase in the number of nodes [53]. As per test results better throughput would be obtained when multiple users interact with the blockchain through a node. A business organization can set up several nodes as Ethereum clients, distributed globally based on the number of potential users and target markets. It was computationally expensive to mine for the requisite ethers to submit more than 0.3 million transactions on the public testnet and the tests conducted provide a real benchmark of the performance of the blockchain through a dapp and a smart contract.

No reliable data is available on the total number of Zakaah donors and the average donations made by them enabling an estimation of the average number of transactions needed per donor. The importance of such an application can be realized from the fact that if an amount equivalent to Zakaah, $192.5 billion [31] is taken from the total wealth of $7.7 trillion dollars of 2043 billionaires in the world [32]. then this has the potential to help 12.3 billion people, which is equivalent to 1.77 times more than the world's population. In the absence of requisite data, the optimum approach is to use the Zakaah dapp in a small geographical region limiting the number of users to gather usage statistics by employing the proposed asynchronous transaction submission mechanism till an optimization for Proposition II is reached.

[31] calculations done using data from 24

[32] Pollock, D. (2018). The Fourth Industrial Revolution built on blockchain and advanced with AI. https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-blockchain-and-advanced-with-ai/#7a756b94242b, accessed September 15, 2019

"Bitcoin isn't currently practical for very small micropayments. Not for things like pay per search or per page view without an aggregating mechanism, not things needing to pay less than 0.01. The dust spam limit is a first try at intentionally trying to prevent overly small micropayments like that."

Satoshi Nakamoto

8

Blockchain-based Micropayment Systems: Economic Impact and Case Studies

The envisaged benefits of blockchain includes the divisible nature of a cryptocurrency, that can facilitate payments in fractions of a cent, enabling micropayments through the blockchain. Micropayments are a critical tool to enable financial inclusion and to aid in global poverty alleviation. This chapter is divided into three units. Unit I conducts a study on the economic impact of blockchain-based micropayment systems, emphasizing their significance for socioeconomic benefit and financial inclusion. The unit also highlights the contribution of blockchain-based micropayments to the cybercrime economy, indicating the critical need of economic regulations to curtail the growing threat posed by the digital payment mechanism. Unit II of the chapter conducts a study of Stellar blockchain platform as a micropayment system, highlighting the drawbacks that impedes it's progress. It elaborates on the technical and non-technical characteristics of Stellar as a micropayment system, while comparing it with the micropayment platforms from Bitcoin and Ethereum. The chapter analyzes a subset of transaction records in Stellar to give an overview of network activity on micropayments and also highlights the economic significance of blockchain-based micropayments. However, scalability and throughput issues plague the technology and prevent it's mass scale adoption. Unit III of the chapter discusses Lightning Network, the off-chain, scalable and high throughput payment solution from Bitcoin. A comparison is conducted to highlight the fee incurred for payment transactions through Lightning Network, Raiden, Stellar, Bitcoin and conventional payment systems to assess its viability as a blockchain-based payment system. The unit also provides an analysis of the data of Lightning Network, to give a global overview of its usage and reachability.

The units in this chapter are as follows:

1. **Unit I: Economic Impact** (See Section 8). This unit deals with the economic impact of blockchain-based micropayments systems including the effect on cybercrimes.

2. **Unit II: Stellar Case Study** (See Section 8.5). This unit focuses on the feasibility of Stellar as a blockchain-based micropayment system. The unit also includes an analysis of payment data in Stellar transactions. The work uses a characterization model to classify the characteristics of blockchain-based micropayment systems.

3. **Unit III: Lightning Network Case Study** (See Section 8.10). This unit sheds light on Lightning Network, the off-chain scaling solution from Bitcoin and does a comparative review of its transaction fees to assess its viability as a payment system. The payment transfers are in the cryptocurrency BTC, which is divisible to extremely small denominations, and hence the study is applicable to it assessment as a micropayment system too. Data analysis of Lightning Network is also highlighted.

The work done in the units enlisted above are all pioneers in the domain and provide a mechanism to gauge the viability of other micropayment systems utilizing cryptocurrency payment transfers in a blockchain network.

Unit I: Economic Impact

8.1 Introduction

Micropayments come in the category of electronic payment systems, which are financial transactions that take place through an electronic medium without using paper checks or cash. A micropayment is a financial transaction involving an amount of money less than a dollar or even a fraction of a cent but a definite number has not been agreed upon as a standard beyond which payment values fall into micropayments as seen in the nomenclature assigned in related literature [126, 112]. High transaction fees is seen as a limiting factor for conducting micropayments by conventional payment solutions and practical implementations to bring about a seamless deployment of micropayments below a dollar, still remains an area of research. Information economy, dominated by the presence of digital goods like blog posts and digital services like online newspapers, has ushered a new era of payments, that involve very small amounts. Micropayments provide the tool to harness the economic benefits that can be reaped from such a market.

Blockchain-based micropayment systems employ the use of cryptocurrencies to facilitate payments and as such are susceptible to all risks and provide all benefits that come in the domain of cryptocurrencies. However, being facilitators of micropayments, some additional beneficial impacts are observed which can aid in the economic progress of the society. The usage of these systems in dark markets and cybercrime has been discussed in Section 8.4. The blockchain platform being used also has an impact on the micropayment system's economic viability. Micropayment systems employing proof of work consensus incur high energy consumption costs and are economically limiting [26], making the platforms unsustainable for long term usage. However, the advent of blockchain platforms using other consensus mechanisms have provided a remedy to this undesirably high utilization of electricity, paving the way for economically viable blockchain-based micropayment systems.

This work is a pioneer in analyzing the economic impact of blockchain-based micropayment systems. The unit gives the relevant background and related work in Section 8.2. The unit discusses economic impact in different facets of the economy in Section 8.3, while the implications for the cybercrime economy are elaborated in Section 8.4. Conclusion is given in Section 8.5.

8.2 Background and Related Work

A micropayment provider can reduce the transaction fee to facilitate payments of small amounts. Apple launched the iTunes store in which songs are sold for 99 cents and Google Play also enabled micropayments as low as 10 cents per song. Both technology giants, Apple and Google, handle these micropayments by employing a probabilistic model for user behaviour to pick an optimal time to balance credit risk versus transaction fee by batching several consumer purchases into one. Cryptocurrencies are digital assets that are used for conducting payments in blockchain platforms and they can be used to develop micropayment systems that enable payments in fractions of a cent. The divisibility property of cryptocurrencies aids in conducting micropayments and a low cost/ nearly zero transaction fee model adopted by a blockchain platform can help to position it as a blockchain-based micropayment system. Lightning Network, Raiden and Stellar are few examples of blockchain-based micropayment systems. However, the use of these systems is presently limited on account of the technological issues and an absence of explicit regulations to govern the usage of cryptocurrencies [141], as in cases of loss of funds there is no redressal mechanism to compensate the users.

Chohan elaborates on the monetary role cryptocurrencies can play in hyperinflation [38]. Nica et al. discuss the economic benefits and risks of cryptocurrencies [141]. Fry and Cheah use econophysics models to examine shocks and crashes in cryptocurrency markets [65]. Li and Wang discuss the technology and economic determinants of the Bitcoin exchange rate [121]. Budish focuses on the economic limits of Bitcoin, indicating skepticism and caution about large-scale uses of the technology [26]. The present work deals with a study of the economic impact of blockchain-based micropayment systems, including the adverse contribution of such systems to cybercrimes.

8.3 Impact on the Economy

8.3.1 Socioeconomic Benefit

The world can be divided into four income groups [164]. There are approximately 1 billion people in Level 1 that live on less than $2 a day, who do not have even the basic necessities of life. Level 2 contains 3 billion people surviving on $2 to $8 a day. Level 3 has 2 billion people, whose needs encompass around $8 to $32 per day. Level 4 has 1 billion people living on more than $32 a day [164]. When we think of payment systems, it is clear that the mainstream financial organizations and payment systems do not cater to people in Level 1 and Level 2, which together make more than half the present worlds' population. The rare who do cater like PayPal, have a fee structure which makes it infeasible to send amounts in fractions of a cent [1]. The people in Level 1 and Level 2 can certainly benefit from donations less than a dollar. Thus, from a socioeconomic perspective and to aid in the achieving of a few Sustainable Development Goals of United Nations Development Program [2], blockchain-based micropayment systems are a breakthrough in being able to transfer fractions of a cent, in real time and at extremely low cost, if not free.

8.3.2 Revenue Generation

The feasibility of micropayments brought about by blockchain-based systems can aid in further development of the market of microproducts [188], where products cost less than a few dollars. The development of e-commerce, virtual goods, online games, digital advertising, social networks and sale of digital information has revamped the need for low fee-based, instant payment transfers of small amounts. If no intermediaries are involved in the process, then this further helps to make this alternative market more independent. Stellar involves anchors but it's extremely low cost transactions and use of blockchain make it a much better technology for micropayments than existing micropayment systems. Global mobile app revenue in 2016 was $88 billion and it is expected to grow to $189 billion

[1] PayPal. (2019). Buying something with PayPal. https://www.paypal.com/uk/webapps/mpp/paypal-fees, accessed May 2, 2019.

[2] United Nations Development Programme. (2012). Sustainable Development Goals. http://www.undp.org/content/undp/en/home/sustainable-development-goals.html, accessed May 10, 2019.

by 2020 [3]. App revenues are mostly generated by advertising and in-app purchases that involve micropayments. When Apple introduced the micropayment pricing model in 2009, then by 2017 around 50% of mobile app revenue was generated through in-app purchases involving amounts of the order of $0.99, $1.99 and $2.99. These new products and market can add to the revenue generation of an economy.

8.3.3 Elimination of Foreign Exchange and Enhancement of Stability

Cryptocurrencies like BTC, from Bitcoin blockchain platform, are seen as commodity money [4], which are deemed to be comparatively more transparent indicating any tampering done with it. Commodity money strengthens the social obligations of the issuer with respect to the wider society dependent on that currency [84] . Further commodity money has long been associated with price stability [21]. Consequently Forex traders have been observed to secure their funds in BTC during periods of volatility to hedge against the instability of fiat currency. Stellar's native cryptocurrency, XLM, is inflationary and is developed more to integrate the blockchain platform into the existing fiat system as opposed to Bitcoin and Ethereum, who seek to provide a more stable monetary system, where a commodity serves as the anchor to stabilize. In the absence of government regulations, cryptocurrencies have witnessed very high fluctuations being used mainly for speculation and investment. A sound regulatory environment and a well-designed cryptocurrency has the potential to be a global digital currency, eliminating the need for foreign exchange. Research is ongoing towards this end as seen in stablecoins [5].

[3] Dogtiev, A. (2018). App Revenues (2017). http://www.businessofapps.com/data/app-revenues/, accessed May 10, 2019.

[4] CNBC. (2018). Virtual currencies are commodities, US judge rules. https://www.cnbc.com/2018/03/07/cryptocurrencies-like-bitcoin-are-commodities-us-judge-rules.html, accessed May 10, 2019.

[5] @onlineBitMEX Research. (2018). A brief history of Stablecoins (Part 1), https://blog.bitmex.com/a-brief-history-of-stablecoins-part-1/, accessed May 10, 2019.

8.3.4 Effect on Monetary Policy

Bitcoin was recognized to be private money by the German government [6]. In an economic system where private money issue is permitted, the nature of optimal monetary policy changes significantly [195]. Fiat money is inconvertible and cannot be redeemed whereas private money like Bitcoin can be redeemed in outside money. Even amidst frictions in the functioning of the private banking system, private money allows for the intermediation of investment whereas fiat currencies do not, making private money superior to fiat [194]. Besides private money has the property to be elastic and it's quantity can respond to shocks in a way that a stock of fiat currency cannot [195]. On account of the above reasons, it can be envisaged that with scalability and low transaction costs, private money like a cryptocurrency, has the possibility to be used in transactions involving goods, instead of fiat currency [188].

8.3.5 Financial Inclusion

The world presently has around 1.7 billion financially excluded adults. According to statistics provided by FINCA International, 76% of the poorest people, in 20 countries across Africa, Eurasia, Latin America, the Middle East and South Asia, are financially excluded [7]. Blockchain-based micropayment systems can provide to people in the lower income group, Level 1 and Level 2, to have access to a means of payment for buying microproducts as well as to store, send and receive payments of small amounts in their community. It can prove to be an alternative for banking services for the lower strata of society. An increasingly high number of people are relying on e-payments in the world. However, the value of a card payment, in nominal terms, has declined over the last decade and a half, from over $60 to less than $40. The smallest average value of a card payment was around $8 in 2016 [15] but card-based payments have no well-defined standard to cater to micropayments, leaving an unexploited avenue. Blockchain-based micropayment systems can fill this gap while accelerating the process of financial inclusion.

[6] Clinch, M. (2013). Bitcoin recognized by Germany as 'private money'. https://www.cnbc.com/id/100971898, accessed May 11, 2019.

[7] Graham, S. (2018). The 2017 Global Findex: A fresh look at reaching the unbanked. https://finca.org/blogs/2017-global-findex-a-fresh-look/, accessed May 11, 2019.

8.4 Contribution to the Cybercrime Economy

The economic definition of money implies usage of a currency as a unit of account, a medium of exchange and a store of value [141]. However, cryptocurrencies have been majorly used as a store of value, serving as assets for speculative purposes and as investment instruments. Their usage as a medium of exchange has been observed majorly in dark markets and online vendors selling illegal goods [141]. Blockchain-based micropayment systems use cryptocurrencies as a medium of exchange and pose the threat of being used as enumerated above with the additional risk of being used in micro-laundering. Cybercrime economy is generating a minimum revenue of $1.5 trillion per annum with illicit and illegal online markets contributing to approximately $860 billion annually to the revenue [130]. Digital payments like PayPal are being used to engage in micro-laundering techniques [161]. So far, cryptocurrencies account for only 4% of money laundered, which is equivalent to $80 billion per year [130], but they remain a potential medium for further growth of this economy. Blockchain-based micropayment systems like Lightning Network and Raiden, which provide the facility of conducting multiple micropayments without the payment transactions being recorded on the main blockchain platform can only serve to further this economy in the future. Cybercriminals reinvest the money in illegal trafficking of drugs, terrorist activities and further cybercrime. Economic regulations and adequate Anti-Money laundering/ Combating the Financing of Terrorism (AML/ CFT) measures need to be implemented to target this growing threat posed by all digital payments.

8.5 Conclusion

In this unit, we conducted a study on the economic impact of blockchain-based micropayment systems and highlighted the contribution of such systems to the cybercrime economy. An analysis of the economic impact indicates that the low cost micropayment model provided by blockchains can serve to reach the underbanked, expanding the cryptocurrency user base. These systems can aid in poverty alleviation by facilitating donations of a few dollars, with the blockchain ensuring that the funds reach the intended recipients. Blockchain-based micropayment systems can promote the development and increase the revenue stream, from the microproducts market. The absence of regulations has made cryptocurrencies vulnerable for exploitation in illegitimate uses. A study of the contribution of such digital payment mechanisms to the cybercrime economy brings out the critical need for the formulation and implementation of economic regulations and preventive laws, to intercept and disrupt cybercrime.

Unit II: Stellar Case Study

8.6 Introduction

Information economy, dominated by the presence of digital goods like blog posts and digital services like online newspapers, has ushered a new era of payments, that involve very small amounts. Micropayments provide the tool to harness the economic benefits that can be reaped from such a market. Bank of America charges around $30 for outgoing domestic wire transfers and $35 for outgoing international wire transfer sent online in foreign currency [8]. The pricing model would make the transaction fee higher than the micropayment itself. PayPal charges 5% of the product cost and 5 cents for micropayments [9]. Thus, a dedicated micropayment provider can bring down the transaction fees to make micropayments feasible.

In this unit, we conduct a case study on Stellar blockchain and compare its characteristics as a micropayment system with Lightning Network, from Bitcoin and Raiden, from Ethereum. Bitcoin and Ethereum are the pioneers in blockchain technology. Stellar was released in April 2015 by the Stellar Development Foundation and was initially brought into conception in 2014 by McCaleb and Kim. Lightning Network is a second-layer network, that functions on top of the Bitcoin blockchain network. Raiden is an off-chain scaling solution from Ethereum blockchain that facilitates payment transfers using ERC20 compatible tokens. The extremely low cost transactions in the payment solutions under consideration makes them usable for the micropayments use case. The unit gives the related work in Section 8.7. It provides a brief description of Stellar, an overview of it's drawbacks

[8] Bank of America. Advantage Plus Banking. Overview of key policies and fees, 2019. https://www.bankofamerica.com/content/documents/deposits/service/pdf/docrepo/BofA_CoreChecking_en_ADA.pdf

[9] PayPal Inc. Buying something with PayPal, 2019. https://www.paypal.com/uk/webapps/mpp/paypal-fees.

and an analysis of Stellar transactions in Section 8.8. A comparative discussion on the characteristics of Stellar as a blockchain-based micropayment systems is accomplished in Section 8.9. Conclusion of the undertaken study to give a direction for further research in this domain in Section 8.10.

8.7 Related Work

Micropayments have been an active area of research and much effort has gone into analyzing the efficacy of micropayment systems. Ali et al. did an exhaustive survey on the development of different micropayment systems [8]. Pass and Shelat proposed a new lottery-based micropayment scheme for ledger-based transaction systems [151]. Parhonyi et al. discuss the predictability of second-generation micropayment systems at faring better than the first generation systems by recognition of causative agents of failure in the first generation [148]. Lundqvist et al. propose a single fee micropayment protocol using blockchain technology [182]. Our work involves a case study of Stellar as a blockchain-based micropayment system concentrating on its technical and non-technical characteristics, while highlighting the potential issues that impact its usage. The work is a pioneer in providing a discussion on the economic significance of blockchain-based micropayment systems.

8.8 Stellar

Stellar is a blockchain-based payment network, that connects financial organizations and people to provide extremely low cost, cross-border payment transfers within seconds. Stellar conducts payment transfers in its native cryptocurrency, Lumens/ XLM. Anchors in Stellar play the pivotal role of converting the fiat currency into cryptocurrency and serve as bridges between the users and the Stellar network (Figure 8.1). These anchors need to be trustworthy and are generally banks and financial organizations. Stellar also provides a distributed currency exchange which gives the best exchange rate for a certain fiat currency. Stellar blockchain came into inception with the mission to increase access to low cost financial services, to reduce poverty and maximize individual potential. Transactions on the Stellar network get resolved in 3-5 seconds. Tempo, a payment system, utilizes Stellar to send remittances from Europe to the world and 600000 transactions can be executed incurring $0.01 fee,

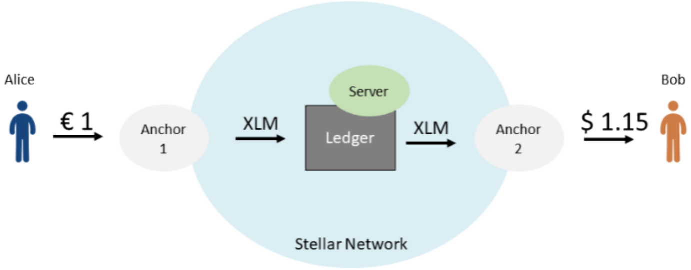


Figure 8.1: Simplified View of a Payment Transfer in Stellar

making Stellar blockchain a very good candidate for micropayment systems [10].

The consensus mechanism used in Stellar is Federated Byzantine Agreement (FBA), which is a generalization of Byzantine agreement [129]. Stellar has a set of designated nodes, known as validator nodes, that participate in the consensus. Any user can be a validator node. Each validator node has a set of nodes that it trusts. When a consensus is reached in the network then this implies that a majority of the validator nodes in the network, as well as a majority of the nodes, that each validator node trusts are in agreement. Stellar supports smart contracts like Ethereum, though they are limited in functionality comparatively.

Stellar users need to have a certain minimum balance in their Stellar accounts before they can transfer money. Sending a payment is an operation in Stellar and a group of operations with additional information on the payer account and signature constitute a transaction. If one operation in a transaction fails, then all fail. Every operation has a base fee of 100 stroops, which is 0.00001 XLM. Stroop is the smallest unit of XLM. The transaction fee is determined by the base fee multiplied by the number of operations. It is independent of the payment amount and the number of hops in the payment route. An account can perform only one transaction at a time and every account has a sequence number, which helps to verify the order of transactions. The asset being sent through the payment needs to be specified. The native currency, XLM, other cryptocurrencies like BTC and fiat currencies like dollar for example, are permitted. In Stellar the amount of asset being sent is represented as a string to accommodate very small values and do away with the inaccuracies introduced by floating point

[10] Stellar Network Overview. https://www.stellar.org/developers/guides/get-started/

mathematics.

8.8.1 Potential Issues

Stellar blockchain platform suffers from some drawbacks, listed below, which limit its throughput and usage:

1. Stellar depends on the need to trust anchors and thus, is not a true representative of a blockchain network, that upholds a distinguishing feature of absolving the need to trust intermediaries for conducting payments.

2. Stellar charges even for those payments that fail to execute making the users pay for failed transactions. For example, a requirement in Stellar is to have a certain minimum number of XLM in each user account, without which a payment transfer would not go through. If a user sends a payment thereafter, it would fail with the user incurring fees [11].

3. Stellar nodes have a transaction limit, thus restricting the throughput of the network. Transactions that are not included are held for a future ledger, when few transactions are waiting [12].

8.8.2 Analysis of Stellar Blockchain Data on Payments

We analyzed 140,000 transaction records in Stellar, which involved some kind of asset transfer. The data, dates of transactions and scripts used can be accessed from the repository[13]. The reviewed data contained operations of the type 'payment', 'path_payment' and 'create_account'. Payment operations, where the same asset is delivered to the receiver as sent by the payer, dominated and accounted for 98,282 transactions. Path payment operations, where the asset sent can differ from the one received, utilizing the decentralized exchange of Stellar, accounted for 5709 transactions. Operations 'create_account' create and fund the account with the specified XLM, accounted for the remaining

[11] Stellar/ go. Transactions that fail during consensus are ignored by Horizon. https://github.com/stellar/go/issues/309

[12] See 10

[13] GitHub Link for Stellar Data. https://github.com/nidakhanlu/micropayments-blockchain

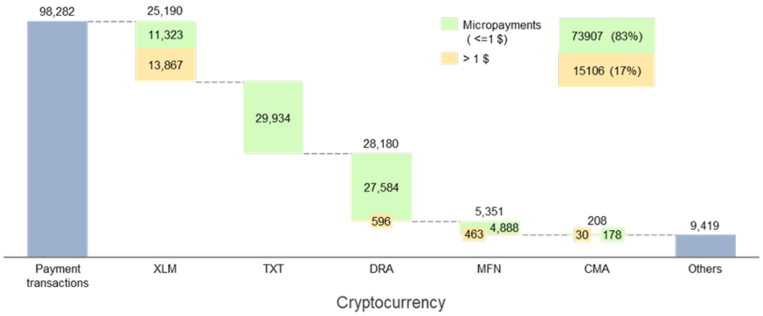


Figure 8.2: Depiction of Micropayment Transactions in Stellar Payments with The Cryptocurrency

transaction records. We took micropayments to be less than/ equal to US $1 for our analysis. The exchange rates employed correspond to 30th March, 2019 and it must be noted that the value of cryptocurrencies is volatile.

Figure 8.2 depicts a waterfall chart of the total payment transactions, where the major cryptocurrencies that dominated the transactions in being utilized for payment transfers are indicated. The transactions in each listed cryptocurrency are further categorized into micropayment transfers and others. The listed cryptocurrencies, XLM, TXT, DRA, MFN and CMA accounted for 90.42% of the payment transactions, whereas all other cryptocurrencies accounted for the remaining. Among the 90.42% of the payment transactions, 83% were in the category of micropayments.

Figure 8.3 depicts the payment transactions, grouped into major fee categories, in decreasing order. The figure also shows variation in the payment amounts with the transaction fee incurred and lists down the variation for 74.1% of the analyzed 'payment' transaction records. It is observed that most of the payment transactions fall in the category of micropayments, in all the categories of transaction fee depicted. A major reason for this might be that most of the payment transactions, as seen in Figure 8.2, were conducted using cryptocurrencies, whose exchange rates in USD were low at the time of computation. It is observed that both low and high transaction fee categories are composed majorly of micropayments. Stellar transaction fee is independent of the payment amount but increases with the increase in transaction complexity, measured by the number of operations in the transaction. Both simple and complex transactions constitute micropayments in payment transactions with the incurred transaction fees less than a cent.

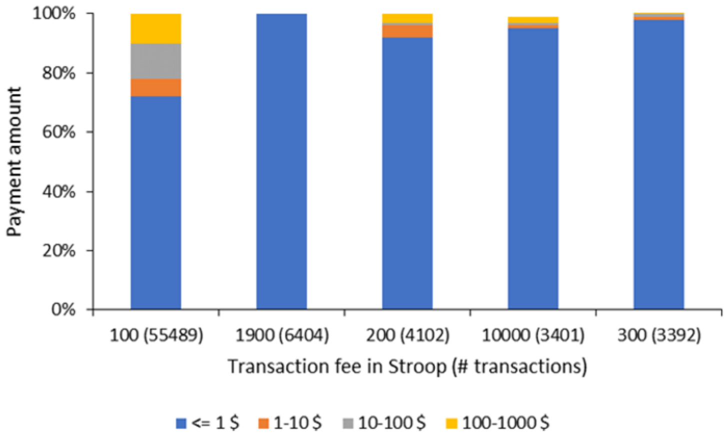


Figure 8.3: Payment Transactions - Variation of Transaction Amounts in Major Fee Categories

Figure 8.4 depicts the major transaction fee categories, that were paid for 76.4% of the analyzed 'path_payment' records. The number of transactions conducted, incurring that particular fee amount, are indicated alongside. It can be observed that a transaction fee of 100 stroops had 50% of the transactions in the category of micropayments, a fee of 200 stroops had 40% and a fee of 5216 stroops had only 10%. A higher transaction fee of 8000 stroops had no micropayment transactions. It can be concluded that micropayment transactions in path payments are less in complexity in terms of the number of operations.

8.9 Characteristics of Stellar as a Micropayment System

Academic literature on micropayment systems have suggested several characterization models for classifying and evaluating micropayment systems. Kniberg [112] in 2002 presented a list of characteristics, while Abrazhevich [1] in 2001 classified micropayment systems on the basis of user and technology-related characteristics. This work uses the characterization model espoused by Weber in 1998 and classifies them into two groups, namely technical and non-technical.

Micropayment systems have witnessed two phases of innovation [149], initiated by the emergence of the first generation of micropayment systems in 1994, which failed by the end of 1990's. They were succeeded by the second generation systems in 1999-2000, with some of these micropayment systems

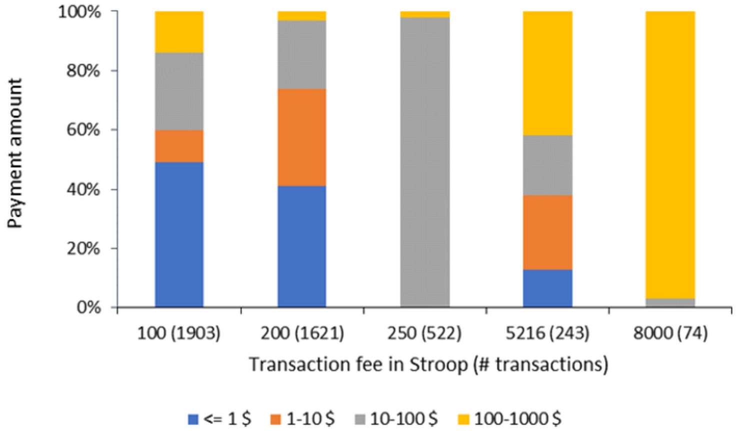


Figure 8.4: Path Payment Transactions - Variation of Transaction Amounts in Major Fee Categories

persisting till today. The first generation systems provided a lot of information on the technical characteristics of the systems whereas the second generation focused on the non-technical characteristics.

The discussion lists down most of the characteristics sufficient to help in reaching a conclusion on the undertaken study but is not exhaustive and is a comparative review of Stellar, Lightning Network and Raiden from the perspective of blockchain-based micropayment systems. Lightning Network facilitates extremely low and even zero cost transactions between the payer and the receiver through a network of payment channels, in the cryptocurrency of Bitcoin, BTC [154]. The technology in Raiden [24] is comparable to Lightning Network and is based on state channel technology. The payment transfers in Lightning Network and Raiden can be either direct, subject to the availability of a payment channel between the transacting entities, or indirect, facilitated through intermediaries connecting the two entities.

8.9.1 Technical

The technical characteristics of a system depend on the underlying technology used and hence the focus is on the functionality and architecture of the systems under study.

1. Medium of Exchange. This defines whether the payment transfer is through a digital currency, fiat money or tokens. Stellar conducts payment transfers only in it's native cryptocurrency

XLM. Bitcoin's Lightning Network enables micropayment transfers directly in BTC, whereas Ethereum's Raiden facilitates payment transfers in ERC20 tokens.

2. Anonymity of Users. Lightning Network and Raiden both preserve the anonymity of users, whereas Stellar is pseudonymous. The anchors have the identity of the users and transactions can be traced back to them.

3. Scalability. Stellar presently has a throughput of 1000+ transactions per second with 1 billion accounts [14]. Stellar has integrated payment channels similar to Lightning Network to enhance it's scalability [15]. Lightning Network is capable of scaling to billions of transactions per second and Raiden is capable of achieving a throughput equivalent to Lightning Network.

4. Ease of Use. Stellar, Lightning Network and Raiden need a certain degree of technical awareness for users to be able to use it. Blockchain-based micropayment systems are similar to first generation of micropayment systems in this context, which were difficult for an average user for making payments on account of their technical complexity [148].

5. Validation. This property determines whether an online contract with a third party is required for payment transfer. This is always true for Stellar for all exchanges except in XLM. It is also true for both Lightning Network and Raiden for payment transfers through intermediaries.

6. Security. Security is evaluated here on the basis of payment delivery in the midst of fraud. Stellar employs standard public-key cryptography using Ed25519 algorithm [46] and recommends offline storage of secret seed, by which the public-private key pair for Stellar account is generated. Lightning Network has in-built security through timelocks whereas Raiden through smart contracts and hashlocked payment transfers. Every user on the reviewed networks has a blockchain account protected by a public-private key pair. Theft of the private key would make the systems under study vulnerable.

[14] Stellar Community. Stellar- Uniqueness/ Differentiation – II, 2018. https://stellarcommunity.org/t/stellar-meetup-in-singapore/1665/2

[15] Starlight, https://github.com/interstellar/starlight

7. Latency. Micropayments should be conducted within a reasonable amount of time. Stellar conducts a payment transfer on the main blockchain network within 3-5 seconds. Lightning Network can facilitate micropayments in seconds within a payment channel but if a payment channel needs to be opened/ closed then each action would require a minimum of 10 minutes (30). Raiden works on the same principle as Lightning Network and a token can be transferred in seconds within a payment channel if a Token Network exists. However if a Token Network does not exist then, creating a Token Network will take a minimum of 14 seconds and opening or closing of a payment channel thereafter would additionally take 14 seconds each (30). This time would increase in periods of network congestion.

8. Interoperability. This implies users of one system can transfer a payment to another system in another currency. Stellar supports interoperability between both fiat and cryptocurrencies. Lightning Network permits transactions across blockchains if the other blockchain supports the same hash function to allow for secure transactions without a third party. Raiden also permits atomic swaps but so far both Lightning Network and Raiden are limited to interoperability between cryptocurrencies and not fiat currency.

8.9.2 Non-Technical

These characteristics deal with the usability of the system from the users' context.

1. Privacy. In Stellar the anchors need to ensure regulatory compliance and have access to user data. Personal and payment information is not available for public review in Lightning Network and Raiden except for the total amount transferred to the user account in the end. The users are known by their underlying Ethereum or Bitcoin address.

2. Geographical Outreach. This determines the geographical region within which the system can be used. Stellar, Lightning Network and Raiden are available for international users.

3. Market Penetration. This determines the total number of users of the system under study.

Stellar has 1 million active user accounts in a span of 3 years [16]. Lightning Network has approximately 7614 nodes within nearly a year of it's launch on the Bitcoin mainnet [17]. An alpha version of Raiden went live on the Ethereum mainnet at the end of 2018 but it is not yet production ready [18] to enable an estimation of it's market penetration.

4. Prepaid or postpaid. The systems under study entail buying of the native cryptocurrencies to transact and hence all come in the category of prepaid micropayment systems. All payments less than or equal to the funds in a user's account, subject to the existence of a path supporting the payment transfer in the network, are executed.

5. Trust. This deals with the confidence users have in the capability of the system as well as to bearing of risks by the service provider. All risks are borne by the users in the systems under study. For example if funds are stolen from the users account or en route a payment transfer, the liability would be with the user. Trust towards these systems presently is low and hence mass adoption is not observed.

6. Payment Threshold. Stellar, Lightning Network and Raiden have no lower limit for conducting payment transfers bounded only by the users' intention with respect to the fees that would be incurred. However, in Lightning Network and Raiden, there is a practical limit on the upper bound to which a payment can be conducted. Lightning Network and Raiden have payment channels through which the payment is routed and channels should have sufficient capacity in available funds to conduct the transfer.

8.10 Conclusion

The study of Stellar indicates that it facilitates payments in seconds and is energy efficient, since there is no mining. Stellar data analysis indicates that the transaction fee is equivalent to less than a cent

[16] Jorn Van Zwanenburg. Stellar achieves milestone of 1 Million active accounts, 2018. https://www.investinblockchain.com/stellar-1-million-accounts.

[17] Lightning Network search and analysis engine, accessed March 25, 2019. https://1ml.com/

[18] Muriuki, W. Raiden Network goes live on Ethereum making 1 Million transactions per second a reality, 2018. https://www.coinspeaker.com/raiden-network-ethereum/

for all analyzed transactions. Payment transactions (70.2%) dominate, in contrast to path payments (4.1%), in the analyzed records. It was observed that the majority of the payment transactions are micropayments (83%), whereas path payments transactions comprise of a more diverse mix of payment amounts. A comparative study of the characteristics as a micropayment system indicates that Stellar fares well in terms of providing on-chain payments. Stellar also provides support for regulatory compliance and AML/ KYC procedures through integration of the compliance protocol [19], preventing the usage of XLM in cybercrime, with a compromise on the absolving of intermediaries in blockchain. However, Stellar requires more focus on the non-technical characteristics of micropayment systems to expand it's user base and increase trust.

[19] Compliance Protocol. https://www.stellar.org/developers/guides/compliance-protocol.html

Unit III: Lightning Network Case Study

8.11 Introduction

Lightning Network was launched to solve the scalability and performance issues in Bitcoin and is an off-chain network that runs parallel to the Bitcoin blockchain. Bitcoin was conceptualized as a peer to peer payment network in a paper by Satoshi Nakamoto in 2008 [138]. At present Bitcoin supports 7 transactions per second [20] with a block size limit of 1 MB and a blockchain size of 235.29 GB [21]. If block size limit was increased to replace all other global financial transactions through Bitcoin, then the entire network would collapse or at the most lead to extreme centralization of Bitcoin nodes to the economically privileged. Further the storage requirements for the increased block size as well as the bandwidth requirements would be beyond the capabilities of home computers making Bitcoin lose it's utility for the masses. In order to scale the Bitcoin network, it was concluded that the transactions need to be off the Bitcoin blockchain [154]. Thus, the inception of Lightning Network took place to have a throughput of nearly unlimited number of transactions per second with very low fees.

Lightning Network was developed as a payment solution serving as an alternative to Bitcoin and seeks to cater to micropayments as well. Micropayments is a domain that has not been exploited and still remains an area of untapped potential [8]. Lightning Network can serve as a payment solution for digital goods and services, where the costs are very low, ranging in the micropayments domain, and negligible transaction fees can be an advantage. It can also facilitate faster and cheaper cross-border transaction flows as compared to traditional payment methods. The present work is a pioneer in conducting both a comparative review of whether Lightning Network is a viable payment solution or not, using transaction fees as the evaluating parameter, and an analysis of its data to give an estimate of its

[20] Stellar Community. Stellar- Uniqueness/ Differentiation – II, 2018. https://stellarcommunity.org/t/stellar-meetup-in-singapore/1665/2

[21] BitInfoCharts, Cryptocurrency Statistics. https://bitinfocharts.com/, accessed January 28, 2019

usage and reachability. The unit gives the background and related work in Section 8.12. A comparison of the fee incurred for payment transactions through conventional and blockchain-based payment solutions is given in Section 8.13. Analysis of Lightning Network data is given in Section 8.14, while the conclusion is provided in Section 8.15.

8.12 Background and Related Work

Lightning Network is a second layer payment network developed on top of the Bitcoin blockchain platform. Theoretically it consists of an infinite number of bidirectional payment channels between users and can be used with other blockchain platforms too. A payment channel allows two transacting entities to do as many transactions as desired off-chain with only the initial and final transactions being recorded on the Bitcoin blockchain, incurring transaction fees. Hence, the fee for multiple off-chain transactions is the same as the fee for two transactions on Bitcoin. A payment channel is required for two entities to conduct payment transfers, the creation of which incurs high fee (Table 8.1). However, Lightning Network also facilitates payment transfers through an intermediary in the network, who has payment channels with the two entities. This feature is extended by incorporating multiple intermediaries in the network to conduct a payment transfer from one entity to another leading to a web of payment channels. The intermediary charges a very low fee for providing the payment channel (Table 8.1). The payment channels utilize multisignature [22] technology and locktime [23] to ensure a secure payment transaction without the need to trust the other party and the intermediaries, if involved. Lightning Network employs onion routing to securely and anonymously route payments within the network [24]. Sampolinsky and Zohar proposed the GHOST rule [175] offering performance benefits over the longest chain rule in Bitcoin. In [190], a brief overview of emerging directions in scalable blockchains is given with a discussion on the proof of work and Byzantine Fault Tolerant consensus mechanisms. Burchert et al. proposed an addition of a third layer to Bitcoin to function as an en-

[22] Bitcoin Wiki, Multisignature, https://en.bitcoin.it/wiki/Multisignature, accessed January 2, 2019.

[23] Bitcoin.org, Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide#term-locktime, Accessed January 4, 2019.

[24] GitHub Lightning Network, Onion routed micropayments for the Lightning Network, https://github.com/lightningnetwork/lightning-onion, accessed January 10, 2019.

hancement for the second layer, Lightning Network, as a means to bring about cost reduction and scalability [27]. Prihodko et al. proposed a new payment routing algorithm for Lightning Network [155]. Roos et al. proposed a decentralized routing for path-based transaction networks, like Bitcoin and Ethereum [163]. Pass and Shelat put forward a new lottery-based scheme for micropayments for ledger-based transaction systems [151]. This work involves data analysis of Lightning Network and a comparative review of the transaction fees to evaluate it's potential to become a feasible payment solution.

8.13 Comparison of Transaction Fees

Lightning Network was released to serve as a scalable low cost payment solution but it provides less secure transactions than Bitcoin [154]. Hence, the following discussion evaluates the costs of payment transfers of small amounts of $1 from Alice to Bob and 50 cents from Alice to David through it. It compares the cost incurred with similar payment transfers through Raiden, Stellar, Bitcoin, MasterCard, Bank of America and PayPal. The fees are reflected in US dollars in Table 8.1 to facilitate an easy comparison between the different payment systems. The fee incurred in the relevant cryptocurrency is indicated alongside. The conversion rate used is applicable for a specific day [25]. The cryptocurrency value and the transaction fee in blockchains is volatile. Hence, the indicated costs in dollars would change accordingly.

8.13.1 Lightning Network

Lightning Network functions by registering the transactions to open and close a payment channel on the Bitcoin blockchain. Alice and Bob need to set up a payment channel between them to send some BTC, the cryptocurrency of Bitcoin. They deposit funds, $3 each in BTC, to open a channel and thereafter broadcast this deposition, which gets recorded on the Bitcoin blockchain. The payment transfers through the opened payment channel cannot exceed the deposited funds, which is referred to as the channel capacity. In our analysis, we consider the transaction fee needed to include the trans-

[25] Bitcoin transaction fees, https://bitcoinfees.info/, accessed January 29, 2019.

action in the next block of Bitcoin (10 minutes), which is 18 satoshis/ byte (satoshi is the smallest unit of bitcoin cryptocurrency)[25]. Thereafter, Alice can send BTC equivalent to $1 to Bob accomplishing a direct payment transfer and close the payment channel. The procedure can be repeated in parallel with David to send 50 cents to him. The total fee and time for direct payment transfers in Table 8.1 indicates the costs and time for above. In the case of a payment transfer through an intermediary, let us assume that Bob already has a payment channel with David and Alice opens a payment channel with Bob. Alice sends $1 in BTC to Bob and 50 cents in BTC to David, through the payment channel of Bob paying the channel fee to him and closes the channel. The channel fee is 1 satoshi [26]. Table 8.1 gives the total fee and time for payment transfers from Alice to Bob and from Alice to David with Bob as intermediary in mediated payments. The lower bound of the transfer time is indicated and it can increase in periods of network congestion. The '+' sign used in the total time for payment transfers indicates a few seconds more. Similar payment transfers can be accomplished in Bitcoin through two transactions as seen in Table 8.1.

8.13.2 Raiden

Raiden Network [27] is the off-chain scaling solution for Ethereum blockchain network [197]. Ethereum provides the feature of smart contracts. Raiden helps in instant, low fee payment transfers based on ERC20 tokens. ERC20 is a token standard, which describes the functions and events that an Ethereum token contract has to implement. The payment process is similar to Lightning Network and payment channel technology is employed to enable low cost, bidirectional payments. The transacting entity needs to have ERC20 tokens in an address, which needs to be registered with Raiden. Once registered by deploying a Token Network Contract on Ethereum, a token has a Token Network associated with it and the Token networks are responsible for opening new payment channels between transacting entities. If a transacting entity needs to send a payment transfer in an ERC20 token, which is already registered, then the costs for registering the token are absolved. The payment process after

[26] Coindesk News, You can now get paid (a little) for using Bitcoin's Lightning Network, https://www.coindesk.com/you-can-now-get-paid-a-little-for-using-bitcoins-lightning-network, accessed January 28, 2019.

[27] Raiden Homepage, The Raiden Network. https://raiden.network/, accessed January 28, 2019.

registration is akin to Lightning Network where the transacting entity needs to open a payment channel with another only if there are no intermediaries connecting them by depositing some tokens. As before the payment transfers through the channel cannot exceed the deposited tokens. The costs for token registration on Ethereum is 3.5 million gas [28], where gas is the unit to measure computational effort needed to execute an operation on the Ethereum Virtual Machine to calculate the costs in Ether (ETH), the cryptocurrency of Ethereum. We consider the fastest time the transaction can be included in Ethereum similar to our consideration for inclusion in the next block of Bitcoin for Lightning Network and it costs 0.091 ETH or $9.55[29]. The mean time for transaction confirmation is presently 38 seconds [29] whereas theoretical limit was 14 seconds [20]. Data for channel fee is not available but it is predicted to be so low that the overall fee would not be affected significantly by its inclusion. The transaction cost for open and closing the payment channel in Ethereum for fastest transaction time with 21000 gas is 0.0005 ETH [29]. In Table 8.1 the costs and time for the given payment transfers from Alice for both unregistered and registered token are depicted. The first row in both *Direct* and *Mediated* represent the fees for unregistered token whereas the second row represent the fees for registered token. The cost for registration is 0.091 ETH. The methodology for fee computation for the payment transfers is the same as in Lightning Network. A mediated transfer includes the channel fee assumed as $0.

8.13.3 Stellar

Stellar is an open-source, distributed, blockchain-based payments infrastructure. Stellar aids in the optimum conversion of fiat currency into cryptocurrency, XLM, to enable fast cross-border payments between different currencies at extremely reduced rates between people, payment systems and financial organizations [30]. Sending a payment is an operation in Stellar and every operation has a base fee of 10-5 XLM [30]. The transaction fee depends upon the base fee and the number of operations. When a transacting entity conducts a payment transfer of some XLM to another, then a default fee is charged

[28] Raiden GitHub, Getting started with the Raiden API, https://raiden-network.readthedocs.io/en/stable/api_walkthrough.html

[29] ETH Gas Station, https://ethgasstation.info/calculatorTxV.php, accessed January 29, 2019.

[30] Stellar, https://www.stellar.org/developers/, accessed January 29, 2019.

(Table 8.1). The default fee is independent of the amount transferred with the transfer time being 3-5 seconds [20]. Table 8.1 depicts the total fee and time for direct and mediated payments from Alice to Bob and David in Stellar.

8.13.4 Conventional Payment Methods

We consider payment transfers through a few popular payment solutions like PayPal, bank transfer through Bank of America and MasterCard. The transfer time varies from a few hours to several days in conventional payment methods. Since the amount is low, micropayment rates of PayPal would apply, which are 5% + $0.05 [31] of the paid amount. Payment transfers of $1 and 50 cents would therefore incur a total cost of $0.175. Bank of America charges $30 for a domestic wire transfer and more for international money transfers [24] so payments of $1 and 50 cents through a similar bank is not feasible. The credit card company MasterCard has a payment transaction fee of 0.19% + 0.53 [32] of the transacted amount in United States, which would cost a total fee of $1.063 for payment transfers of $1 and 50 cents.

8.14 Data Analysis of Lightning Network

A beta version of Lightning Network was launched on the Bitcoin mainnet in March 2018 and we extracted data related to Lightning Network nodes, payment channels and channel capacity. Information was extracted concerning node ID, total number of payment channels of a node, total number of open channels and total number of closed channels. Our data collection dates till the first 5 months of its public release and reflects the state of the Lightning Network parameters till that time. In all, it was found that 60 countries have at least one Lightning Network node. We observed that US, which had 1141 nodes, out of the total 1983, owned 57.5% of the nodes. Germany ranked second with 165 nodes and France ranked third with 80 nodes. At the lower rung we had countries like Iceland, Malta, Peru with just one node and Indonesia, Thailand and Chile with 2 nodes.

[31] PayPal, https://www.paypal.com/ca/webapps/mpp/merchant-fees, accessed January 29, 2019.

[32] Bank of America, https://www.bankofamerica.com/foreign-exchange/wire-transfer.go, accessed January 29, 2019.

Table 8.1: Total Transaction Fee and Time for 2 Payment Transfers

Payment system	Lightning Network	Raiden	Stellar	Bitcoin
Open Channel: fee, time	$0.16, (18 satoshi byte), 600s	$0.05, (0.0005ETH), 38s	-	-
Close Channel: fee, time	$0.16, (18 satoshi byte), 600s	$0.05, (0.0005ETH), 38s	-	-
Direct Payment: fee, time	$0, milliseconds to seconds	$0, subseconds	$0.08, ($10^{-5}XLM$), 3-5s	$0.16, (18 satoshi byte), 600s
Channel: fee, time	$0.00003, (1 satoshi), few seconds	very low, few seconds), 600s	-	-
Total: fee, time 1. Direct	$0.64, 1200s+	$9.75, 114s+ $0.20, 76s+	$0.16, 3-5s+	$0.32, 600s
2. Mediated	$0.32003, 1200s+	$9.65, 114s+ $0.10, 76s+	$0.16, 3-5s+	-

Figure 8.5 represents the top 7 countries in decreasing order of the total number of Lightning Network (LN) nodes on the x-axis. The y-axis represents the channel capacity per node per country and is calculated by multiplying the total channel capacity of the country by a factor of k=*1000*. The result is then divided by the total number of nodes in the country. The usage of the factor k is to normalize the data for optimum analysis and visualization. It was observed that US, which had the highest number of nodes, had the lowest channel capacity of 0.0362 BTC per node among the 7 countries. France ranked third in the total number of nodes but had the highest channel capacity of 0.0666 per node.

We also analyzed the total channel capacity of all the nodes found in 60 countries. The mean channel capacity was found to be 1.45, the standard deviation was 5.44 and the variance of the analyzed data was 29.64. The median was found to be at 0.24 BTC, which gives us the channel capacity lying in between the highest of 41.32 BTC of US and 0 BTC of Latvia. Argentina and Greece had a total channel capacity of 0.24 BTC. Three countries Uruguay, Latvia and Iceland had zero channel capacities with no open payment channels.

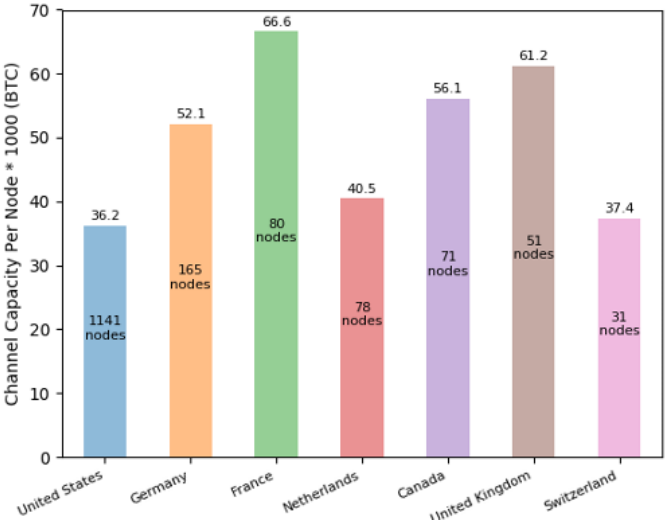


Figure 8.5: Channel Capacity per Node in Countries with the Highest Number of LN Nodes

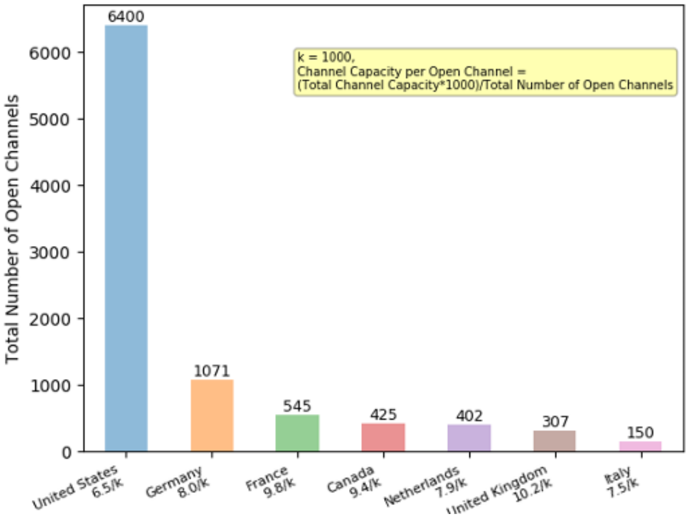


Figure 8.6: Countries with the Highest Number of Open Channels

Figure 8.6 depicts 7 countries, with the highest number of open payment channels with labels on the x-axis giving the channel capacity per open channel in a country. Normalized data is represented in the labels and it needs to be divided by a factor of $k=1000$ to derive the actual channel capacity. It was observed that UK had the highest channel capacity per open channel at 0.0102 BTC whereas US had the lowest at 0.0065 BTC. We also observed the total number of open and closed payment channels per country and it was seen that US has both the highest number of open payment channels at 6400 and the highest number of closed payment channels at 9279.

8.15 Conclusion

In this unit a comparison of the analyzed payment solutions indicates that the fee incurred for a payment transfer through Lightning Network is less than in Raiden (unregistered token), while Stellar provides the fastest payment transfer. Lightning Network and Raiden compute transaction fee based on the number of intermediaries, independent of the amount transferred. Stellar charges a default fee independent of both the payment amount and the number of hops in the network. It is also observed that the utility of Lightning Network lies in conducting multiple payment transfers using intermediaries and Bitcoin would be cheaper to use if only direct payment transfers are involved. PayPal comes close to offering similar transaction fees. Data analysis of Lightning Network reveals that United States is at the forefront of using the technology since it has the highest number of Lightning Network nodes, highest number of open channels and highest total channel capacity for payments. Lightning Network has the potential to become a viable payment solution catering more to the micropayment sector, as the channel capacity restricts the payment amount. Financial institutions as intermediaries to provide liquidity will help to strengthen it as a payment solution. Future work would involve analysis of the data of Raiden to bring about an optimum assessment of the comparison between different blockchain-based payment solutions.

"The measure of greatness in a scientific idea is the extent to which it stimulates thought and opens up new lines of research."

Paul Dirac

9 Conclusion

BLOCKCHAIN IS ***"AN EVOLVING LANDSCAPE"*** WITH THE TRAJECTORY IN THE PAST YEAR INDICATING AN UPWARD TREND CULMINATING IN TANGIBLE STRATEGIC ADVANTAGES in unprecedented ways for organizations [1]. The finance industry and in particular the financial technology domain leads the development in blockchain with other industries treading cautiously. The survey by Deloitte [2] indicates that there was a 40% increase in 2019 as compared to 2018 in the willingness to invest in blockchain with respondents having indicated an investment of US$ 5 million and above in 2019. There was also a 10 point increase, in the same tracking period, in the respondents, who felt that blockchain is a critical priority for their organization, approximating to 53% of the respondents. Additionally around 83% saw potential use cases of blockchain that would propel an organization to

[1] Deloitte Insights. (2019). *Deloitte's 2019 Global Blockchain Survey. Blockchain gets down to business.* https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf, accessed May 12, 2020.

[2] see 1

deploy the technology. There is an overall increase in the trust financial organizations, startups and governments place in the utility of blockchain [3]. The technology has a profound impact on the financial sector [111], limited only by the scalability and throughput issues plaguing the technology [53], preventing a widespread practical realization of the same. The dissertation is a study on the effectiveness of blockchain usage for financial applications with a focus on the envisaged benefits of traceability and immutability characteristics of blockchain. In view of the above, the work elaborated in this dissertation is pivotal in providing a qualitative and a quantitative assessment of the deployment of the technology in financial organizations.

9.1 Contribution to Scientific Research

The main achievements of the research discussed in this dissertation, to the best of our knowledge, are all pioneers in the domain. The research conducted during this period also involved an attempt to resolve the throughput and scalability issues in blockchain by the proposition of a novel blockchain consensus mechanism using MapReduce [125] and Lamport's logical clock [116] in permissioned blockchains networks. The pioneering work [101] was a prototype and received very good reviews by the scientific committee in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, BlockSys@SenSys 2018*. However the proposition could not be tested extensively for robustness and hence a detailed discussion on the same was not included in this dissertation. The primary scientific achievements are reiterated below:

1. Proposition of mathematical formulae to aid in the prediction of the best governance strategy for blockchain networks. In Chapter 3, we analyzed the position of blockchain governance within the hierarchy of Institutional governance to derive a formal structure for blockchain governance. The chapter viewed blockchain governance from the dimensions of IT governance and then analyzed one dimension of IT governance, namely decision-making process as in the form of voting on a new blockchain improvement proposal, by using Nash equilibria to predict optimal governance strategies. A game theory simulation of the respective strategies of the players was used in an attempt to define the most optimum scenarios based on choices made by the voters or the broader community. The chapter, through an analysis of the payoff matrices, proposed mathematical formulae that can predict the occurrence of a hard fork on acceptance/ rejection of a new proposal as well as give an indication whether the majority of the community will move to the upgraded chain or stay on the original chain. The validity of the novel mathematical formulae was verified in the chapter through real Ethereum data. After the DAO hack on Ethereum, there was a proposal to upgrade the chain in 2016. Our proposed formulae accurately predicts the hard fork in Ethereum, which led to formation of Ethereum and Ethereum Classic. Further our formulae also predicts that the payoff will be more with the upgraded chain (Ethereum) as compared to Ethereum Classic, observable from the the present day metrics of the upgraded chain (Ethereum) [3] and the original chain (Ethereum Classic) [4]. The work is a pioneer in defining blockchain governance in an interdisciplinary context and giving a mathematically sound framework for a financial organization to aid in the decision-making process, when confronted with different voting scenarios on an improvement proposal.

2. **Novel usage of smart contracts in a management plane for monitoring and management of blockchain-based applications through the desired administrative hierarchy.** In Chapter 4, we designed, implemented and evaluated a management plane for both smart contracts and smart contract-based decentralized applications. Two services have been instantiated in this plane which are data filtering for access control and data monitoring of deployed smart contracts. We build a monitoring tool to display public blockchain data using a dashboard coupled with a notification mechanism of any changes in private data to the administrator of the monitored decentralized application.The two services could be applied using a one-to-one or one-to-many management strategies for interacting with the managed contracts. This can be utilized in financial organizations, using decentralized applications/ smart contracts, to replicate the existing administrative practices emanating from a central unit by using our proposed one-to-many management strategy. The management of different departments within an organization by the department heads can be replicated using our proposed one-to-one management strategy.

3. **Design, implementation and evaluation of a novel privacy management plane using differ-**

[3] CoinMarketCap. (2019). Ethereum (ETH). https://coinmarketcap.com/currencies/ethereum/, accessed December 15, 2019.

[4] CoinMArketCap. (2019). Ethereum Classic (ETC). https://coinmarketcap.com/currencies/ethereum-classic/ratings/, accessed December 15, 2019.

ential privacy to ensure adherence to GDPR. In Unit II of Chapter 5 we designed, implemented and evaluated a novel privacy management plane. The work is a pioneering step towards achieving GDPR compliance through the blockchain using differential privacy, managed through smart contracts. The developed privacy management plane facilitates data curators to allow queries on their data through a decentralized application with the query results being stored on the blockchain. The storage of query results on the blockchain paves the way for multiple usage of the results without compromising on the integrity of the result and absolves the need for repetition of the same query by others. The privacy management plane also demonstrated the integration of local differential privacy with the individual data owners selecting the level of data perturbation and controlling the privacy budget through a blockchain-based decentralized application. The privacy management plane was extended by integrating the work in Chapter 4. As a result, the privacy management plane was enhanced upon to include management by another smart contract as a preventive mechanism for restricting read access to a data record stored on the blockchain. This enhancement when used in a permissioned blockchain network will ensure the data owner's right to revoke his permission for sharing his data. The developed decentralized application to achieve local differential privacy can be used by organizations to collect perturbed data, giving the users the right to control the privacy of their data with the data being stored off the blockchain if needed and queried in a global privacy context through the blockchain. The implementation is a basic step towards ensuring data privacy and compliance to GDPR.

4. **Novel, exploratory and conceptual analysis of tokenization of investment certificates through a smart contract.** In Chapter 6, we coded a basic smart contract to gauge the contract development complexity and effort required for tokenization of Sukuk, ethical investment certificates, on Ethereum. The chapter provides a systematic approach to assess and analyse fundamental elements of commercial feasibility of sukuk tokenization. By addressing the fundamental factors of cost-benefit analysis, such as the cost factors of blockchain transactions, and by conceptualising the main findings and concerns of adoption, we provided a solid assessment framework for organizations that intend to tokenize sukuk. Tokenization of sukuk emphasizes on the need for regulations to govern the usage of blockchain.

5. **Pioneer in development and evaluation of a decentralized application utilizing crowdfund-**

ing for donation to resolve key issues related to traceability and transparency. In Chapter 7, we introduce a novel model in the form of a decentralized app designed, developed and deployed on the Ethereum blockchain. The decentralized app solves the challenges present and optimizes the process of donation in a specific obligation of Muslims, namely Zakaah. Load and stress tests on the prototype of the smart contract in the public testnet of Ethereum were analyzed to gauge the feasibility of mass usage. Similar tests were done in Hyperledger to conclude on the optimum blockchain platform for donation. A novel strategy was proposed to enhance the throughput of Ethereum. The testing is a pioneer in evaluating the throughput and feasibility of a blockchain-based financial product and provides a benchmark to validate the business and technical hypotheses of other similar financial products and services. Our conclusion was that Ethereum blockchain is presently not equipped to handle the number of transactions that can take place during the peak month of Zakaah donation, namely the month of fasting.

6. Pioneer in assessing the economic impact of blockchain-based micropayments. In Chapter 8 we conducted a study on the economic impact of blockchain-based micropayment systems and highlighted the contribution of such systems to the cybercrime economy. An analysis of the economic impact indicates that the low cost micropayment model provided by blockchains can serve to reach the underbanked, expanding the cryptocurrency user base. These systems can aid in poverty alleviation by facilitating donations of a few dollars, with the blockchain ensuring that the funds reach the intended recipients. Blockchain-based micropayment systems can promote the development and increase the revenue stream, from the microproducts market. The absence of regulations has made cryptocurrencies vulnerable for exploitation in illegitimate uses. A study of the contribution of such digital payment mechanisms to the cybercrime economy brings out the critical need for the formulation and implementation of economic regulations and preventive laws, to intercept and disrupt cybercrime.

The main achievements of the dissertation are represented graphically in a hypothetical model of a financial ecosystem depicted in Figure 9.1, where the achievements are numbered in the chronological order followed above. The figure depicts that the financial organization deploys the decentralized donation application on a blockchain network. The amount of donation (2.5% as given in Chapter 7) is debited in an automated manner from the bank accounts of the users registered in the donation dapp.

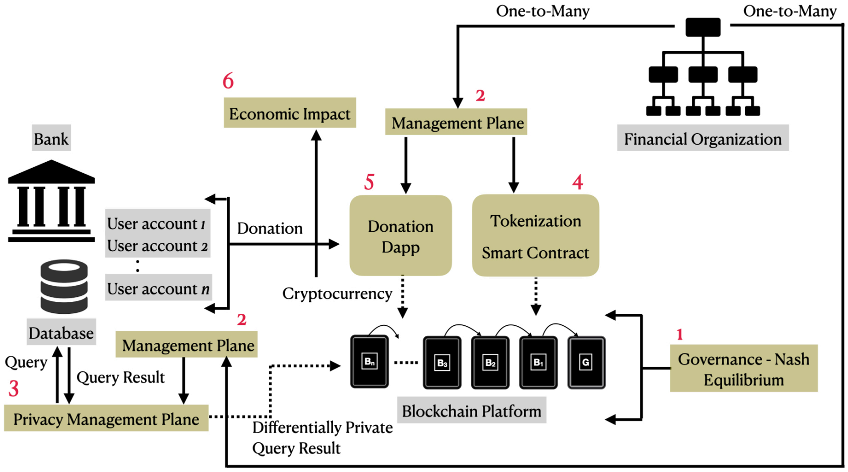


Figure 9.1: Model of a Financial Ecosystem Utilizing the Primary Contributions of this Dissertation

The donation is facilitated using cryptocurrencies for micropayment and payment transactions. The economic impact of the usage of blockchain-based micropayments, discussed in Chapter 8, applies to the scenario. The financial organization also deploys a smart contract for tokenization of investment certificates as elaborated upon in Chapter 6. The donation application and the tokenization smart contract are managed through the management plane developed in Chapter 4 by the department head using one-to-many management strategy. The database of the bank is queried using the privacy management plane developed in Unit II of Chapter 5. The privacy management plane is managed by another smart contract to bring about GDPR compliance using the management plane of Chapter 4 but to ensure compliance, the blockchain platform should be permissioned.. Finally the governance of the entire blockchain network by the financial organization is through the mathematical model that was developed in Chapter 3 using Nash equilibrium.

9.2 Critical Assessment

A critical assessment of the main contributions of this dissertation are enumerated below:

1. **Chapter 3: Governance of Blockchain Networks.** The work proposes mathematical formulae to predict optimal governance strategies applicable to blockchain networks. The formulae

have been verified using real Ethereum data. Ethereum follows an off-chain governance mechanism and a robust testing should involve using the formulae for a blockchain platform with an on-chain governance mechanism as well. Rigorous testing needs to be conducted using data for the diverse scenarios elucidated in the payoff matrices.

2. **Chapter 4: Management Plane for Smart Contracts**. The management plane developed is a prototype, where the smart contract was customized for the blockchain-based applications evaluated in the work. The cost evaluation of these strategies regarding Ether fees and the used gas was conducted only for one-to-many and one-to-one strategy.

3. **Chapter 5 Unit II: Management Plane for Differential Privacy Preservation through Smart Contracts**. In this work, the channel of communication between the web application and the relational database as well as the web application and the decentralized application can be attacked to thwart the privacy. Further, the evaluation was done on the public Ethereum network.

4. **Chapter 6: Tokenization of Investment Certificates**. The work involved conducting a cost-benefit analysis to determine the feasibility of tokenization compared to conventional Sukuk issuance. We used data from a conventional sukuk issuance but the demarcation of the individual cost elements was not given. We used data from World Bank estimates to fill the gap while calculating the costs for tokenization on the public, private and consortium Ethereum blockchain. Thus the resulting cost estimations are approximate. Further, blockchain is still in stages of development and many additional cost factors like security issues, know your customer (KYC), key management and the like enumerated in Section 6.8 were not added to the total cost in conducting the cost-benefit analysis.

5. **Chapter 7: Decentralized Donation Application for a Crowdfunding Platform**. The work was evaluated using public Ethereum blockchain and no tests were conducted on private Ethereum to estimate the feasibility of mass usage. No reliable data was available on the total number of Zakaah donors and the average donations made by them enabling an estimation of the average number of transactions needed per donor.

6. **Chapter 8 Unit I: Blockchain-based Micropayment Systems: Economic Impact**. The economic impact of blockchain-based micropayment systems is a theoretical review and apart from the impact on cybercrime economy, lacks data to strengthen it. The qualitative work is supported by related work in academic literature.

9.3 Future Work

The following enumerates the future work that can enhance the research work in this dissertation:

1. **Chapter 3: Governance of Blockchain Networks**. The work can be enhanced by simulating voting on off-chain and on-chain blockchain platforms' improvement proposals. The simulation should involve exposing the blockchain to the different scenarios of voting on submission of an improvement proposal. The generated data should be analyzed using the proposed formulae. Further real data from all the forks that have occurred, in all the blockchain platforms developed so far, should be categorized into different case scenarios and evaluated to verify the prediction results using our proposed formulae.

2. **Chapter 4: Management Plane for Smart Contracts**. The work should be enhanced by programming a general Solidity library for management that can be utilized to develop the proposed management plane. This will provide more seamless instrumentation functions for smart contracts to integrate monitoring operations with little effort from the developers. Further, investigation and evaluation of the cost of management while varying different factors including monitoring polling frequencies, number of monitored and accessed attributes, etc should be conducted.

3. **Chapter 5 Unit II: Management Plane for Differential Privacy Preservation through Smart Contracts**. The work can be enhanced by developing a more secure mechanism to access the relational database and add Laplace noise. Use of artificial intelligence should be incorporated in the privacy management plane to offer predictions based on the data, while ensuring privacy. The enhanced privacy management plane should be deployed and evaluated in a permissioned blockchain network.

4. **Chapter 6: Tokenization of Investment Certificates**. The work in the chapter should be enhanced by the design, implementation and evaluation of a hybrid arrangement incorporating tokenization with existing issuance models. This hybrid arrangement should take into account the existing regulations. Additionally, a formal model should be given for the legacy system to integrate with blockchain for developing novel structuring methodologies for sukuk tokenization.

5. **Chapter 7: Decentralized Donation Application for a Crowdfunding Platform**. The work should be extended to conduct load and stress tests on private as well as consortium Ethereum blockchain to enable a more just estimation of the viability of the application for mass usage. Donation data on the number of transactions conducted should be acquired from other platforms, outside the function of Zakaah, and a feasibility analysis should be conducted to know the average number of transactions per donor.

6. **Chapter 8 Unit I: Blockchain-based Micropayment Systems: Economic Impact**. The economic impact of blockchain-based micropayment systems should be extended to incorporate a quantitative impact analysis. Relevant data in different domains, indicated to be affected by the usage of cryptocurrencies to conduct micropayments, should be acquired for the same.

References

[1] Abrazhevich, D. (2001). Classification and characteristics of electronic payment systems. In *Proceedings of the Second International Conference on Electronic Commerce and Web Technologies*, EC-Web 2001 (pp. 81–90). Berlin, Heidelberg: Springer-Verlag.

[2] Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7, 56.

[3] Al-Essa, M. (2019). The impact of blockchain technology on financial technology (FinTech). *PhD Thesis for MSc in Business Innovation and Informatics, Università degli Studi di Salerno*.

[4] Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, 2, 287.

[5] Aldar (2020). FY 2019 financial statements. https://www.aldar.com/en/Investor-Relations/Pages/latest-results.aspx, accessed April 17, 2020.

[6] Aldweesh, A., Alharby, M., & van Moorsel, A. (2018). Performance benchmarking for Ethereum opcodes. In *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1–2).

[7] Alharby, M. & van Moorsel, A. (2019). Blocksim: A simulation framework for blockchain systems. *SIGMETRICS Perform. Eval. Rev.*, 46(3), 135–138.

[8] Ali, S. T., Clarke, D., & McCorry, P. (2017). The nuts and bolts of micropayments: A survey. *CoRR*, abs/1710.02964.

[9] Anderson, L., Holz, R., Ponomarev, A., Rimba, P., & Weber, I. (2016). New kids on the block: An analysis of modern blockchains. *CoRR*, abs/1606.06530.

[10] Arrunada, B. & Garicano, L. (2018). Blockchain: The birth of decentralized governance. *Pompeu Fabra University, Economics and Business Working Paper Series, 1608*.

[11] Athey, S., Catalini, C., & Tucker, C. (2017). *The digital privacy paradox: Small money, small costs, small talk*. Technical report, National Bureau of Economic Research.

[12] Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6.

[13] Barrera, C. & Hurder, S. (2018). Blockchain upgrade as a coordination game. *SSRN*. https://dx.doi.org/10.2139/ssrn.3192208.

[14] Bartoletti, M. & Pompianu, L. (2017). An empirical analysis of smart contracts: Platforms, applications, and design patterns. *Lecture Notes in Computer Science*.

[15] Bech, M. L., Faruqui, U., Ougaard, F., & Picillo, C. (2018). Payments are a-changin' but cash still rules. *BIS Quarterly Review*.

[16] Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, 19, 1020–1034.

[17] Berger, C. & Reiser, H. P. (2018). Scaling byzantine consensus: A broad analysis. In *Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, SERIAL'18 (pp. 13–18). New York, NY, USA: Association for Computing Machinery.

[18] Bernstein, D. J., Josefsson, S., Lange, T., Schwabe, P., & Yang, B.-Y. (2015). EdDSA for more curves. *IACR Cryptology ePrint Archive*, 2015, 677.

[19] Biryukov, A. & Khovratovich, D. (2017). Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger*, 2.

[20] Blum, A., Dwork, C., McSherry, F., & Nissim, K. (2005). Practical privacy: The sulq framework. In *Proceedings of the ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems* (pp. 128–138).

[21] Bordo, M., Dittmar, R., & Gavin, W. (2007). Gold, fiat money, and price stability. *Topics in Macroeconomics*, 7, 1525–1525.

[22] Bowe, S., Hornby, T., & Wilcox, N. (2019). Zcash protocol specification. version 2019.0.1 [overwinter+sapling]. https://whitepaperdatabase.com/zcash-zec-whitepaper/, accessed April 24, 2020.

[23] Braggion, E., Gatti, N., Lucchetti, R., & Sandholm, T. (2015). Strong Nash equilibria and mixed strategies.

[24] Brainbot (2018). Raiden specification document, release 0.1. https://media.readthedocs.org/pdf/raiden-network-specification/latest/raiden-network-specification.pdf, accessed October 12, 2019.

[25] Buchman, E. (2016). Tendermint: Byzantine fault tolerance in the age of blockchains. Master's thesis, The University of Guelph. (In partial fulfillment of requirements for the degree of Master of Applied Science in Engineering Systems and Computing).

[26] Budish, E. (2018). The economic limits of bitcoin and the blockchain. *National Bureau of Economic Research*.

[27] Burchert, C., Decker, C., & Wattenhofer, R. (2017). Scalable funding of bitcoin micropayment channel networks - regular submission. In *SSS*.

[28] Castro, M. & Liskov, B. (1999). Practical Byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*.

[29] Chaer, A., Salah, K., Lima, C., Ray, P., & Sheltami, T. (2019). Blockchain for 5G: Opportunities and challenges. In *IEEE Globecom 2019*.

[30] Chase, B. & MacBrough, E. (2018). Analysis of the XRP ledger consensus protocol.

[31] Chauhan, A., Malviya, O., Verma, M., & Singh Mor, T. (2018). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122–128).

[32] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (PoET). In *International Symposium on Stabilization, Safety, and Security of Distributed Systems* (pp. 282–297).

[33] Chen, S., Zhang, J., Shi, R., Yan, J., & ke, Q. (2018). A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems.

[34] Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018). When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 1178–1187).

[35] Chen, Y. & Bellavitis, C. (2019a). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13.

[36] Chen, Y. & Bellavitis, C. (2019b). Decentralized finance: Blockchain technology and the quest for an open financial system. *Stevens Institute of Technology School of Business Research Paper*.

[37] Chiu, J. & Koeppl, T. V. (2019). Blockchain-based settlement for asset trading. *The Review of Financial Studies*, 32(5), 1716–1753.

[38] Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. *Noteson the 21st Century: Critical Blockchain Research Initiative*.

[39] Chutimon Satidularn, Carla Wilkin, K. T. & Linger, H. (2013). Investigation of the relationship between IT governance and corporate governance. *Management, Leadership and Governance*, (pp. 420–423).

[40] Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: foundations, design landscape and research directions. *CoRR*, abs/1608.00771.

[41] Cong, L. W. & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, 32(5), 1754–1797.

[42] Cormode, G., Jha, S., Kulkarni, T., Li, N., Srivastava, D., & Wang, T. (2018). Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, SIGMOD '18 (pp. 1655–1658). New York, NY, USA: Association for Computing Machinery.

[43] Cortier, V. & Smyth, B. (2012). Attacking and fixing Helios: An analysis of ballot secrecy. In *IEEE Computer Security Foundations Symposium – CSF 2011*.

[44] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E., Song, D., & Wattenhofer, R. (2016). On scaling decentralized blockchains. volume 9604 (pp. 106–125).

[45] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, 39, 283–297.

[46] Daniel J. Bernstein, Niels Duif, T. L. P. S. & Yang, B.-Y. (2017). Ed25519: high speed high security signatures. `https://ed25519.cr.yp.to/`, accessed April 28, 2020.

[47] Dannen, C. (2017). Cryptoeconomics survey. In *Introducing Ethereum and Solidity* (pp. 139–147). Berkeley, CA: Springer.

[48] Das, P., Eckey, L., Frassetto, T., Gens, D., Hostáková, K., Jauernig, P., Faust, S., & Sadeghi, A.-R. (2019). Fastkitten: Practical smart contracts on bitcoin. In *IACR Cryptology ePrint Archive*.

[49] Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting governance: The new Institutional economics of distributed ledger technology. *SSRN Electronic Journal*.

[50] Davradakis, E. & Santos, R. (2019). Blockchain, fintechs and their relevance for international financial institutions (EIB working paper 2019/01). *The EIB Economics Department*. https://www.eib.org/attachments/efs/economics_working_paper_2019_01_en.pdf, accessed April 15, 2020.

[51] De Angelis, S., Aniello, L., Lombardi, F., Margheri, A., & Sassone, V. (2017). PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain.

[52] De Filippi, P. & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, 21.

[53] Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2017). Blockbench: A framework for analyzing private blockchains. In *Proceedings of the 2017 ACM International Conference on Management of Data*, SIGMOD '17 (pp. 1085–1100). New York, NY, USA: Association for Computing Machinery.

[54] Dinur, I. & Nissim, K. (2003). Revealing information while preserving privacy. In *Proceedings of the Twenty-second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems* (pp. 202–210).

[55] Duffield, E. & Diaz, D. (2019). Dash: A payments-focused cryptocurrency. https://github.com/dashpay/dash/wiki/Whitepaper, accessed April 24, 2020.

[56] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In S. Halevi & T. Rabin (Eds.), *Theory of Cryptography* (pp. 265–284). Berlin, Heidelberg: Springer Berlin Heidelberg.

[57] Dwork, C. & Nissim, K. (2004). Privacy-preserving data mining on vertically partitioned databases. In M. Franklin (Ed.), *Advances in Cryptology – CRYPTO 2004* (pp. 528–544). Berlin, Heidelberg: Springer Berlin Heidelberg.

[58] Dwork, C. & Roth, A. (2014). The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3–4), 211–407.

[59] ensquad (2018). The Berka Dataset Visualization. https://ensquad.com/2018/06/21/the-berka-dataset-visualisation/, accessed March 15, 2020.

[60] EPRS | European Parliamentary Research Service (2019). Blockchain and the general data protection regulation. Can distributed ledgers be squared with European data protection law? *Scientific Foresight Unit (STOA), PE 634.445*.

[61] Eyal, I., Gencer, A. E., Sirer, E., & Van Renesse, R. (2015). Bitcoin-NG: A scalable blockchain protocol.

[62] Feng, X., Ma, J., Miao, Y., Meng, Q., Liu, X., Jiang, Q., & Li, H. (2018). Pruneable sharding-based blockchain protocol. *Peer-to-Peer Networking and Applications*, 12.

[63] Filippi, P. D. & Mcmullen, G. (2018). Governance of blockchain systems: Governance of and by distributed infrastructure. *(Research Report) Blockchain Research Institute and COALA*.

[64] Friedrichs, O., Jakobsson, M., & Soghoian, C. (2008). The threat of political phishing. *SSRN Electronic Journal*.

[65] Fry, J. & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *Elsevier-International Review of Financial Analysis*, 47, 343–352.

[66] Fujisaki, E. & Suzuki, K. (2007). Traceable ring signature. In *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, volume E91.A (pp. 181–200).

[67] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, 10, 20.

[68] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16 (pp. 3–16). New York, NY, USA: ACM.

[69] Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015). Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15 (pp. 692–705). New York, NY, USA: Association for Computing Machinery.

[70] Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. *IACR Cryptology ePrint Archive*, 2017, 454.

[71] Gill, A. (2008). Corporate governance as social responsibility: A research agenda. *Berkeley Journal of International Law*, 26(2).

[72] Gordijn, J. & Akkermans, J. M. (2003). Value-based requirements engineering: Exploring innovative e-commerce ideas. *Requir. Eng.*, 8(2), 114–134.

[73] Graham, S. (2018). The 2017 global findex: A fresh look at reaching the unbanked.

[74] Greenstein, B. (2018). IoT trends in 2018: AI, Blockchain, and the Edge. https://iot.ieee.org/newsletter/january-2018/iot-trends-in-2018-ai-blockchain-and-the-edge, August 13, 2018.

[75] Griffiths, A. B. & Zammuto, R. F. (2005). Institutional governance systems and variations in national competitive advantage. In *The Academy of Management Review*, volume 30 (pp. 823–842).

[76] Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Communications Magazine*, 56(7), 82–88.

[77] Haddouti, S. E. & Ech-Cherif El Kettani, M. D. (2019). Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1–7).

[78] Hangl, C. (2014). A literature review about the landscape of social finance. *ACRN Journal of Finance and Risk Perspectives*, 3.

[79] Hao, W., Zeng, J., Dai, X., Xiao, J., Hua, Q., Chen, H., Li, K.-C., & Jin, H. (2019). Blockp2p: Enabling fast blockchain broadcast with scalable peer-to-peer network topology. *International Conference on Green, Pervasive, and Cloud Computing (GPC), 2019*, (pp. 223–237).

[80] Hasan, H. R. & Salah, K. (2018a). Blockchain-based proof of delivery of physical assets with single and multiple transporters. *IEEE Access*, 6, 46781–46793.

[81] Hasan, H. R. & Salah, K. (2018b). Proof of delivery of digital assets using blockchain and smart contracts. *IEEE Access*, 6, 65439–65448.

[82] He, X., Machanavajjhala, A., & Ding, B. (2014). Blowfish privacy: Tuning privacy-utility trade-offs using policies. In *Proceedings of the 2014 ACM SIGMOD international conference on Management of data* (pp. 1447–1458).: ACM.

[83] Henriquez, R., Cohen, I., Bitan, N., & Tulbassiyev, K. (2018). Blockchain and business model innovation: Designing a P2P mortgage lending system. *SSRN Electronic Journal*.

[84] Hermele, K. (2014). Commodity currencies vs fiat money: Automaticity vs embedment. *FESSUD-Financialisation, Economy, Society and Sustainable Development*, 37(44 (Working Paper Series)).

[85] Hofmann, E., Strewe, U., & Bosia, N. (2018). *Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation*. Springer.

[86] Holt, C. & Roth, A. E. (2004). The Nash equilibrium: A perspective. In *National Academy of Sciences of the United States of America* (pp. 3999–4002).

[87] Houser, K. & Voss, W. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy? *SSRN Electronic Journal*.

[88] HSBC & Sustainable Digital Finance Alliance (2019). Blockchain: Gateway for sustainability linked bonds. https://www.sustainablefinance.hsbc.com/mobilising-finance/blockchain-gateway-for-sustainability-linked-bonds, accessed April 17, 2020.

[89] Hu, X., Yuan, M., Yao, J., Deng, Y., Chen, L., Yang, Q., Guan, H., & Zeng, J. (2015). Differential privacy in Telco big data platform. *Proc. VLDB Endow.*, 8(12), 1692–1703.

[90] Huang, D., Ma, X., & Zhang, S. (2020). Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 172–181.

[91] Hulett, M. (1975). Privacy and the freedom of Information Act. *Administrative Law Review*, (pp. 275–294).

[92] International Islamic Financial Market (2020). Sukuk reports. https://www.iifm.net/sukuk-reports/, accessed April 17, 2020.

[93] Islamic Markets (2018). Aldar sukuk Ltd usd500 million 4.75% 29-sep-2025 - pricing term sheet. https://islamicmarkets.com/publications/aldar-sukuk-ltd-usd500-million-4-75-29-sep-2025-pricing-term, accessed April 17, 2020.

[94] Islamic Relief Worldwide (2015). Annual report 2015. *Islamic Relief Website*. https://www.islamic-relief.org/annual-reports/, accessed September 26, 2017.

[95] Jain, P., Gyanchandani, M., & Khare, N. (2018). Differential privacy: Its technological prescriptive using big data. *Journal of Big Data*, 5.

[96] John G. Keogh, Laurette Dube, A. R. K. J. H. N. K. & Dean, K. (2020). The future food chain: Digitization as an enabler of society 5.0. *Building the Future of Food Safety Technology, 1st Edition, Blockchain and Beyond*. https://www.elsevier.com/books/building-the-future-of-food-safety-technology/detwiler/978-0-12-818956-6, accessed May 11, 2020.

[97] John G. Keogh, Abderahman Rejeb, N. K. K. D. & Hand, K. J. (2020). Data and food supply chain. Blockchain and GS1 standards in the food chain: A review of the possibilities and challenges. *Building the Future of Food Safety Technology, 1st Edition, Blockchain and Beyond*. https://www.elsevier.com/books/building-the-future-of-food-safety-technology/detwiler/978-0-12-818956-6, accessed May 11, 2020.

[98] Juma'h, A. & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management*, 28.

[99] Kalodner, H., Goldfeder, S., Chator, A., Möser, M., & Narayanan, A. (2017). Blocksci: Design and applications of a blockchain analysis platform.

[100] Karame, G. (2016). On the security and scalability of bitcoin's blockchain. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16 (pp. 1861–1862). New York, NY, USA: Association for Computing Machinery.

[101] Khan, N. (2018). FAST: A MapReduce consensus for high performance blockchains. In *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, BlockSys@SenSys 2018*, BlockSys'18 (pp. 1–6). New York, NY, USA: Association for Computing Machinery.

[102] Khan, N., Ahmad, T., Patel, A., & State, R. (2020a). Blockchain governance: An overview and prediction of optimal strategies using Nash equilibrium. *CoRR*, abs/2003.09241.

[103] Khan, N., Ahmad, T., & State, R. (2019a). Blockchain-based micropayment systems: Economic impact. In *Proceedings of the 23rd International Database Applications Engineering Symposium*, IDEAS '19 New York, NY, USA: Association for Computing Machinery.

[104] Khan, N., Ahmad, T., & State, R. (2019b). Feasibility of Stellar as a blockchain-based micropayment system. In M. Qiu (Ed.), *Smart Blockchain - Second International Conference, SmartBlock 2019, Birmingham, UK, October 11-13, 2019, Proceedings*, volume 11911 of *Lecture Notes in Computer Science* (pp. 53–65).: Springer.

[105] Khan, N., Kchouri, B., Yatoo, N. A., Kräussl, Z., Patel, A., & State, R. (2020b). Tokenization of sukuk: Ethereum case study. *Global Finance Journal*.

[106] Khan, N., Lahmadi, A., Francois, J., & State, R. (2018). Towards a management plane for smart contracts: Ethereum case study. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium* (pp. 1–6).

[107] Khan, N. & Nassar, M. (2019). A look into privacy-preserving blockchains. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1–6).

[108] Khan, N. & Ouaich, R. (2017). Feasibility analysis of blockchain for donation-based crowdfunding of ethical projects. In *Smart Technologies and Innovation for a Sustainable Future. Proceedings of the 1st American University in the Emirates International Research Conference — Dubai, UAE 2017* (pp. 129–139). Springer.

[109] Khan, N. & State, R. (2020). Lightning network: A comparative review of transaction fees and data analysis. In *Blockchain and Applications - International Congress* (pp. 11–18). Cham: Springer International Publishing.

[110] Kirit, N. & Sarkar, P. (2017). Escrowchain: Leveraging Ethereum blockchain as escrow in real estate.

[111] Knezevic, D. (2018). Impact of blockchain technology platform in changing the financial sector and other industries. *Montenegrin Journal of Economics*, 14, 109–120.

[112] Kniberg, H. (2002). What makes a micropayment solution succeed. Master's thesis, KTH Institution for Applied Information Technology.

[113] Kokoris-Kogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016). Enhancing bitcoin security and performance with strong consistency via collective signing. In *Proceedings of the 25th USENIX Conference on Security Symposium*, SEC'16 (pp. 279–296). USA: USENIX Association.

[114] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 583–598).

[115] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 839–858).

[116] Lamport, L. (1978). Time, clocks, and the ordering of events in a distributed system. *ACM Digital Library*, 21, 558–565.

[117] Lansiti, M. & Lakhani, K. R. (2017). The truth about blockchain, Harvard Business Review. https://hbr.org/2017/01/the-truth-about-blockchain, accessed January 4, 2017.

[118] Lasaulce, S. & Tembine, H. (2011). Playing with equilibria in wireless non-cooperative games. In *Game Theory and Learning for Wireless Networks*.

[119] Li, W., Andreina, S., Bohli, J.-M., & Karame, G. (2017a). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297–315).: Springer International Publishing.

[120] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017b). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

[121] Li, X. & Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Elsevier-Decision Support Systems*, 95, 49–60.

[122] Liu, Z., Nguyen, C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C., & Kim, D. (2019). A survey on applications of game theory in blockchain.

[123] Loftus, J., May, A., P. Smart, N., & Vercauteren, F. (2011). On CCA-secure somewhat homomorphic encryption. In *International Workshop on Selected Areas in Cryptography*, volume 7118 (pp. 55–72).

[124] M. Schletz, D. N. & Lee, M. (2020). Blockchain and tokenized securities: The potential for green finance (ADBI working paper). *Tokyo: Asian Development Bank Institute*, (1079). https://www.adb.org/publications/blockchain-tokenized-securities-potential-green-finance.

[125] MacLean, D. (2011). A very brief introduction to MapReduce. http://hci.stanford.edu/courses/cs448g/a2/files/map_reduce_tutorial.pdf, accessed August 12, 2018.

[126] Manasse, M. (1995). The millicent protocols for electronic commerce. In *Proceedings of the First USENIX Workshop on Electronic Commerce, July 11 - 12, 1995, New York, New York, USA* (pp. 117–123).

[127] Manda, V. K. & Yamijala, S. (2019). Peer-to-peer lending using blockchain. *International Journal Of Advance Research And Innovative Ideas In Education*, 6, 61–66.

[128] Mavridou, A. & Laszka, A. (2018). Designing secure Ethereum smart contracts: A finite state machine based approach. In *Financial Cryptography and Data Security* (pp. 523–540).

[129] Mazieres, D. (2016). The stellar consensus protocol: A federated model for internet-level consensus.

[130] McGuire, M. (2018). Understanding the growth of the cybercrime economy. RSA Conference.

[131] Mehar, I., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology*, 21, 19–32.

[132] Mense, A. & Flatscher, M. (2018). Security vulnerabilities in Ethereum smart contracts. In *Proceedings of the 20th International Conference on Information Integration and Web-Based Applications Services*, iiWAS2018 (pp. 375–380). New York, NY, USA: Association for Computing Machinery.

[133] Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The honey badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16 (pp. 31–42). New York, NY, USA: Association for Computing Machinery.

[134] Mohamed, S. & Taitoon, J. A. (2019). Islamic finance development report.

[135] Mohsin, M. & Muneeza, A. (2019). Integrating waqf crowdfunding into the blockchain. In *Fintech in Islamic Finance* (pp. 266–279).

[136] Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An empirical analysis of traceability in the Monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018, 143–163.

[137] Muneeza, A., Arshad, N., & Tajul Arifin, A. (2018). The application of blockchain technology in crowdfunding: Towards financial inclusion via technology. *International Journal of Management and Applied Research*, 5, 82–98.

[138] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, accessed October 14, 2018.

[139] Nam, J.-S. & Yang, H.-S. (2017). A study on improvement of housing bond information relay system using blockchain. *Journal of Digital Convergenc*, 15(8).

[140] Nash, J. (1951). Non-cooperative games. *The Annals of Mathematics*, 54, 286–295.

[141] Nica, O., Piotrowska, K., & Schenk-Hoppe, K. R. (2017). Cryptocurrencies: Economic benefits and risks. *University of Manchester, FinTech working paper no. 2*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856.

[142] Nicta, V. G. (2016). On the danger of private blockchains (when PoW can be harmful to applications with termination requirements).

[143] Nissim, K., Steinke, T., Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., O'Brien, D. R., & Vadhan, S. (2017). Differential privacy: A primer for a non-technical audience. In *Privacy Law Scholars Conf.*

[144] Novotny, P., Zhang, Q., Hull, R., Baset, S., Laredo, J., Vaculín, R., Ford, D., & Dillenberger, D. (2018). Permissioned blockchain technologies for academic publishing. *Information Services Use*, 38, 1–13.

[145] Odiljon, A. & Gai, K. (2019). *Efficiency Issues and Solutions in Blockchain: A Survey*, (pp. 76–86).

[146] Okamoto, T. & Ohta, K. (1992). Universal electronic cash. In J. Feigenbaum (Ed.), *Advances in Cryptology — CRYPTO '91* (pp. 324–337). Berlin, Heidelberg: Springer Berlin Heidelberg.

[147] Oliveira, M. T., Carrara, G. R., Fernandes, N. C., Albuquerque, C. V. N., Carrano, R. C., Medeiros, D. S. V., & Mattos, D. M. F. (2019). Towards a performance evaluation of private blockchain frameworks using a realistic workload. In *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)* (pp. 180–187).

[148] Parhonyi, R., Nieuwenhuis, B., & Pras, A. (2006). *The Fall and Rise of Micropayment Systems*. Springer.

[149] Párhonyi, R., Nieuwenhuis, L. J. M., & Pras, A. (2005). Second generation micropayment systems: lessons learned. In M. Funabashi & A. Grzech (Eds.), *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government* (pp. 345–359). Boston, MA: Springer US.

[150] Parm Sangha, V. P. & Soman, S. (2020). Advancing global trade with blockchain: How to unleash value from trusted, interconnected marketplaces. *IBM Research Insights*.

[151] Pass, R. & Shelat, A. (2015). Micropayments for decentralized currencies. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 207–218).: ACM.

[152] Patel, A. (2015). Channeling asset-managed sukuk towards SMEs financing : Sukuk mudaraba prototype applied to a french SME. *European Journal of Islamic Finance*.

[153] Patrick B. G. van der Wansem, L. J. & Rivetti, D. (2019). Issuing international bonds: A guidance note. *World Bank Group (Discussion Paper)*. http://documents.worldbank.org/curated/en/491301554821864140/pdf/Issuing-International-Bonds-A-Guidance-Note.pdf.

[154] Poon, J. & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

[155] Prihodko, P., Zhigulin, S., Sahno, M., Ostrovskiy, A., & Osuntokun, O. (2016). Flare : An approach to routing in Lightning Network white paper.

[156] Puad, N. A. M., Rafdi, N. B. J., & Shahar, W. S. S. (2014). Issues and challenges of waqf instrument : A case study in MAIS. In *E-proceedings of the Conference on Management and Muamalah (CoMM 2014)*.

[157] Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. *IEEE Access*, 7, 148550–148575.

[158] Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in blockchain technologies and social contract theories. *Ledger*, 1, 134–151.

[159] Richard D. McKelvey, A. M. M. & Turocy, T. L. (2014). Gambit: Software tools for game theory. http://www.gambit-project.org, accessed December 12, 2019.

[160] Richard-Marc Lacasse, B. L. & Khan, N. (2018). Islamic banking - Towards a blockchain monitoring process. *Journal of Business and Economics*. https://revues.imist.ma/index.php?journal=jbe&page=article&op=view&path%5B%5D=13448, accessed May 11, 2020.

[161] Richet, J. (2013). Laundering money online: a review of cybercriminals methods. *CoRR*, abs/1310.2368.

[162] Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, 18(4).

[163] Roos, S., Moreno-Sanchez, P., Kate, A., & Goldberg, I. (2018). Settling payments fast and private: Efficient decentralized routing for path-based transactions. In *Network and Distributed Systems Security (NDSS) Symposium*.

[164] Rosling, H., Ronnlund, A. R., & Rosling, O. (2018). *Factfulness: Ten Reasons We're Wrong About the World–and Why Things Are Better Than You Think*. New York: Flatiron Books.

[165] Rouhani, S. & Deters, R. (2017). Performance analysis of ethereum transactions in private blockchain. In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (pp. 70–74).

[166] Rouhani, S. & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, 7, 50759–50779.

[167] Rudnyckyj, D. (2018). *Beyond Debt: Islamic Experiments in Global Finance*, (pp.74).

[168] Saberhagen, N. V. (2013). Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf, accessed April 24, 2020.

[169] Salah, K. & Hasan, H. (2018). Blockchain-based solution for proof of delivery of physical assets. In *2018 International Conference on Blockchain (ICBC 2018)*.

[170] Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, 7, 10127–10149.

[171] Simonsson, M. & Johnson, P. (2005). Defining IT governance – a consolidation of literature. In *EARP Working Paper MS103*.

[172] Singh, A., Parizi, R., Zhang, Q., Choo, K.-K. R., & Dehghantanha, A. (2019). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers Security*, 88, 101654.

[173] Smith, S. (2019). Blockchain, tokenization, and implications for financial services practitioners. *International Journal of Accounting and Financial Reporting*, 9, 1.

[174] Solé, J. (2008). Prospects and challenges for developing corporate sukuk and bond markets© international monetary fund.: Lessons from a kuwait case study. *International Journal of Islamic and Middle Eastern Finance and Management*, 1, 20–30.

[175] Sompolinsky1, Y. & Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. *Financial Cryptography and Data Security-19 thInternationalConference*.

[176] Suliman, A., Husain, Z., Abououf, M., Alblooshi, M., & Salah, K. (2019). Monetization of IoT data using smart contracts. *IET Networks*, 8(1), 32–37.

[177] Sulin Ba, J. S. & Whinston, A. B. (2001). Introducing a third dimension in information systems design: The case for incentive alignment. *Information Systems Research*, 12, 225–239.

[178] Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing blockchains: Characteristics applications. In *1th IADIS International Conference on Information Systems*.

[179] Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).

[180] The World Bank (2019). Understanding poverty. https://www.worldbank.org/en/topic/poverty/overview, accessed February 2020.

[181] Thomas Cook, A. L. & Lee, J. H. (2017). *DappGuard: Active Monitoring and Defense for Solidity Smart Contracts*. Technical report, MIT.

[182] Thomas Lundqvist, A. d. B. & Andersson, H. R. H. (2017). Thing-to-thing electricity micro payments using blockchain technology. *Global Internet of Things Summit (GIoTS)*.

[183] Tieman, M. & Darun, M. (2017). Leveraging blockchain technology for halal supply chains. *Islam and Civilisational Renewal*, 8, 547–550.

[184] Turnbull, S. (2008). *Corporate Governance: Theories, Challenges and Paradigms*, volume 1. London: SAGE Publications.

[185] Ul Hassan, M., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, 97.

[186] Uzsoki, D. & Guerdat, P. (2019). Tokenization of infrastructure: A blockchain-based solution to financing sustainable infrastructure. *International Institute of Sustainable Development*.

[187] Vadhan, S. (2017). The complexity of differential privacy. *Information Security and Cryptography*, (pp. 347–450).

[188] Valdes-Benavides, R. A. & Hernandez-Verme, P. L. (2014). Virtual currencies, micropayments and monetary policy: Where are we coming from and where does the industry stand? *Journal of Virtual Worlds Research*, 7(3).

[189] Varga, E. & Hayday, M. (2016). A recipe book for social finance: A practical guide on designing and implementing initiatives to develop social finance instruments and markets. *European Commission, Directorate-General for Employment, Social Affairs and Inclusion*. Luxembourg: Publications Office of the European Union.

[190] Vukolic, M. (2015). The quest for scalable blockchain fabric: Proof-of-Work vs. bft replication. In *iNetSeC*.

[191] Wang, S. (2019). Performance evaluation of hyperledger fabric with malicious behavior. *International Conference on Blockchain (ICBC) 2019*, (pp. 211–219).

[192] Wang, W., Ying, L., & Zhang, J. (2016). On the relation between identifiability, differential privacy, and mutual-information privacy. *IEEE Transactions on Information Theory*, 62(9), 5018–5029.

[193] Weill, P. & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston: Harvard School Press.

[194] Williamson, S. D. (1998). Private money. In *Role of Central Banks in Money and Payments Systems*, Federal Reserve Bank of Cleveland Conference (pp. 469–499).

[195] Williamson, S. D. (2004). Limited participation, private money, and credit in a spatial model of money. *Economic Theory*, 24(4), 857–875.

[196] Wolfram Elsner, Torsten Heinrich, H. & Grabner, C. (2014). Special issue: Aspects of game theory and Institutional economics. In *Games*, volume 5 (pp. 188–190).

[197] Wood, G. (2015). Ethereum: A secure decentralized generalized transaction ledger eip-150 revision. https://gavwood.com/paper.pdf, accessed April 30, 2020.

[198] Xin, W., Zhang, T., Hu, C., Tang, C., Liu, C., & Chen, Z. (2017). On scaling and accelerating decentralized private blockchains. In *2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids)* (pp. 267–271).

[199] Yakubov, A., Shbair, W. M., Khan, N., State, R., Medinger, C., & Hilger, J. (2020). Blockpgp: A blockchain-based framework for PGP key servers. *International Journal of Networking and Computing*, 10(1), 1–24. http://www.ijnc.org/index.php/ijnc/article/view/217.

[200] Yang, M., Margheri, A., Hu, R., & Sassone, V. (2018). Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud Computing*, 5(6), 69–79.

[201] Yermack, D. (2017). Corporate Governance and Blockchains*. *Review of Finance*, 21(1), 7–31.

[202] Zaka, F. & Shaikh, S. (2019). *Blockchain for Islamic Financial Services Institutions*, (pp. 241–262).

[203] Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance (DeFi), IIEL issue brief 02/2020; european banking institute working paper series 59/2020; university of hong kong faculty of law research paper no. 2020/010. *SSRN Electronic Journal*.

[204] Zhao, W., Jin, S., & Yue, W. (2019). *Analysis of the Average Confirmation Time of Transactions in a Blockchain System*, (pp. 379–388).

[205] Zhong, L., Wang, H., Xie, J., Qin, b., Liu, J., & Wu, Q. (2019). *A Flexible Instant Payment System Based on Blockchain*, (pp. 289–306).

[206] Zhou, T., Li, X., & Zhao, H. (2019). Dlattice: A permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization. *IEEE Access*, 7, 39273–39287.

[207] Zhu, Y., Song, X., Yang, S., Qin, Y., & Zhou, Q. (2018). Secure smart contract system built on SMPC over blockchain. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1539–1544).

[208] Zulkhibri, M. (2015). A synthesis of theoretical and empirical research on sukuk. *Borsa Istanbul Review, Elsevier*, 15.

[209] Zyskind, G., Nathan, O., & Pentland, A. (2015a). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184).: IEEE.

[210] Zyskind, G., Nathan, O., & Pentland, A. (2015b). Enigma: Decentralized computation platform with guaranteed privacy. https://arxiv.org/pdf/1506.03471.pdf, accessed April 6, 2020.

This thesis was typeset employing LaTeX, originally developed by Leslie Lamport and based on Donald Knuth's TeX. The body text is set in 11 point Egenolff-Berner Garamond. The image depicted on this page is the *tree of knowledge*, which is the dissertation author's visualization of research spreading light everywhere. Research is perceived as a growing tree with fruits as candles giving off the light of knowledge. A template that can be used to format a PhD dissertation similar to this look & feel has been released under the permissive AGPL license, and can be found online at github.com/suchow/Dissertate or from its lead author, Jordan Suchow, at suchow@post.harvard.edu. The original template was customized for this dissertation and the present work is not a typical representative of the template released under the AGPL license.