6-13-2023

Cross-Blockchain Technology for an Interoperable and Scalable Digital Contact Tracing

Farbod Behnaminia
University of Windsor

Recommended Citation

Behnaminia, Farbod, "Cross-Blockchain Technology for an Interoperable and Scalable Digital Contact Tracing" (2023). *Electronic Theses and Dissertations*. 9313.
https://scholar.uwindsor.ca/etd/9313

Cross-Blockchain Technology for an Interoperable and Scalable Digital Contact Tracing

By

Farbod Behnaminia

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science
at the University of Windsor

Windsor, Ontario, Canada

2023

Cross-Blockchain Technology for an Interoperable and Scalable Digital Contact Tracing

By

Farbod Behnaminia

APPROVED BY:

____

M. Hassanzadeh
Department of Electrical and Computer Engineering

____

D. Alhadidi
School of Computer Science

____

S. Samet, Advisor
School of Computer Science

May 17, 2023

DECLARATION OF CO-AUTHORSHIP / PREVIOUS PUBLICATION

I. Co-Authorship

I hereby declare that this thesis incorporates material that is result of joint research, conducted under the supervision of Dr. Saeed Samet (Advisor). In all cases, the key ideas, primary contributions, experimental designs, data analysis and interpretation, were performed by the author, and the contribution of co-author was primarily through the proofreading of the published manuscripts.

I am aware of the University of Windsor Senate Policy on Authorship, and I certify that I have properly acknowledged the contribution of other researchers to my thesis and have obtained written permission from each of the co-author(s) to include the above material(s) in my thesis.

I certify that, with the above qualification, this thesis, and the research to which it refers, is the product of my own work.

II. Previous Publication

This thesis includes two original papers that have been previously published in journals for publication, as follows:

Chapter	Full Citation	Publication Status
Chapters 1 – 2	Behnaminia, F. , Samet, S. (2023). 'Blockchain Technology Applications in Patient Tracking Systems Regarding Privacy-Preserving Concerns and COVID-19 Pandemic'. International Journal of Information and Communication Engineering, 17(2), 144 - 156.	Published
Chapters 3 – 4	2023 5th Blockchain and Internet of	Submitted

	Things Conference (BIOTC 2023). It will be held in Osaka, Japan during July 21-23, 2023. All peer-reviewed and accepted papers, after presentation, will be published in the ACM International Conference Proceedings (ISBN: 979-8-4007-0821-3)	

I certify that I have obtained a written permission from the copyright owner(s) to include the above published material(s) in my thesis. I certify that the above material describes work completed during my registration as a graduate student at the University of Windsor.

III. General

I declare that, to the best of my knowledge, my thesis does not infringe upon anyone’s copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

The COVID-19 pandemic has highlighted the importance of contact tracing as a tool for controlling the spread of the virus, but it has also raised concerns about the privacy and security of personal information. Blockchain technology, with its immutability and security features, has the potential to address these concerns. However, traditional blockchain solutions may not be sufficient to protect sensitive personal information, especially when it comes to interoperability with other chains that may have different privacy standards.

Cross-blockchain technology, such as the interoperability feature of the Polkadot network, allows for the creation of a decentralized and distributed contact tracing system that can be used by multiple organizations and jurisdictions while ensuring privacy. This research examines the technical challenges and potential solutions of using cross-blockchain technology for interoperable and scalable digital contact tracing. In this research, we proposed a solution using the Polkadot network, where the personal and contact information is stored on a blockchain, accessible only to authorized parties. The use of cross-blockchain technology and encryption would ensure that sensitive personal information is protected and that only authorized parties can access the data. Additionally, the data on the private blockchain would be shareable with other health authorities or other blockchain networks by using the interoperability feature of the Polkadot network.

Overall, this thesis seeks to demonstrate the potential benefits and limitations of using cross-blockchain technology for digital contact tracing applications and highlights the importance of further research and development in this area by providing recommendations for implementing this technology. With the right approach, it is possible to create a contact tracing solution that is both effective and respects the privacy of individuals.

DEDICATION

Dedicated to Elnaz, Leila, Alireza

ACKNOWLEDGEMENTS

I would like to express my sincerest gratitude to my supervisor, Dr. Saeed Samet, for his immense support throughout my graduate studies. Thanks to his plenty of guidance, encouragement, and advice. This thesis would not have been possible without his patience and valuable guidance.

I would like to thank my thesis committee members, Dr. Dima Alhadidi and Dr. Mohammad Hassanzadeh, for taking the time to review my thesis and attending my thesis proposal and defense sessions. Thanks to their guidance and valuable suggestions for improving this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS/SYMBOLS

DLT	Distributed Ledger Technology, an umbrella term that includes blockchain and other similar technologies
SDK	Software Development Kit, a collection of tools and resources that developers use to build software applications
API	Application Programming Interface, a set of protocols and tools for building software applications
IoMT	The Internet of Medical Things (IoMT) refers to the network of medical devices, wearable sensors, and other healthcare technology that are connected to the internet and are able to collect, transmit, and analyze healthcare data in real time.

NOMENCLATURE

Blockchain	A distributed ledger technology that allows for secure and transparent transactions without the need for intermediaries.
Cross-blockchain	A cross-chain solution connects two or more blockchains to transfer digital assets and information seamlessly.
Contact Tracing	The process of identifying and monitoring individuals who may have come into contact with an infected person.
Blockchain Interoperability	The idea of enabling distinct blockchain networks to interact and integrate, communicating seamlessly to allow for the sharing of data between chains.
Scalability of Blockchain	The ability of that platform to support increasing load of transactions, as well as increasing the number of nodes in the network.
Polkadot	A blockchain platform and cryptocurrency. It is designed to allow blockchains to exchange messages and perform transactions with each other without a trusted third-party.
Privacy Preserving	Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service providers or apps, all while allowing marketers to maintain the functionality of data-driven systems.
Patient Centricity	Putting the patient first in an open and sustained engagement of the patient to respectfully and compassionately achieve the best experience and outcome for that person and their family.

CHAPTER 1

Introduction & Background

Digital Contact Tracing (DCT) is a method for using blockchain technology to record and track close contacts between individuals while protecting their personal information. The use of cross-blockchain technology, such as the interoperability feature of the Polkadot network, allows for the creation of a decentralized and distributed contact tracing system that can be used by multiple organizations and jurisdictions. DCT could be used as a tool to help slow the spread of infectious diseases and assist in contact tracing efforts. The topic is a rapidly evolving field of study, and researchers and academics in the fields of public health, computer science, and blockchain technology may be interested in studying and understanding the implications of this technology. Companies and developers working in the field of blockchain technology may be interested in exploring the potential uses of cross-blockchain technology for DCT. Government agencies responsible for public health and privacy protection may be interested in understanding how DCT using cross-blockchain technology, could be used to assist in contact tracing efforts while also protecting individuals' personal information.

This research could contribute by identifying ways to standardize and improve interoperability between different blockchain networks, making it easier for them to work together seamlessly. The ability to slow the spread of infectious diseases while also protecting individuals' personal information and privacy is of great importance. Research in this area is valuable because it has the potential to make a real-world impact, advance the field of blockchain technology, protect individuals' personal information and privacy, and help navigate the legal and economic challenges that this technology raises.

To provide the context of the study, we are going to have a solid start and cover foundations. On December 31st, 2019, the World Health Organization (WHO) was alerted about instances of pneumonia of unknown etiology in Wuhan City, China. Authorities in China announced the discovery of a new coronavirus, which they named “2019-nCoV,” on January 7, 2020. Infectious disorders caused by Coronaviruses (CoV) range from the common cold to more severe conditions. Humans have not before been infected with a novel coronavirus (nCoV). In an effort to promptly discover any new 2019-nCoV cases, countries throughout the world have ramped up their monitoring. When it comes to secure data exchange, blockchain is becoming a safe and efficient network. This includes applications in the financial and healthcare industries. Blockchain has the potential to transform the healthcare industry. Confidential and authorized data can be exchanged securely through this method. In a blockchain consortium, any healthcare organization can share medical information independently of the system it uses for its native electronic health record [1].

Blockchain

Blockchain is a distributed, peer-to-peer database that accurately and securely records transactions using cryptography so that they may be checked afterwards. The Bitcoin blockchain is a public record of all Bitcoin transactions ever made. Every 10 minutes, a new block is added to the blockchain to record the most recent transactions. The blocks on the blockchain are added sequentially. As soon as a miner connects to the Bitcoin network, he or she is given access to the blockchain, which is instantly downloaded when the miner joins the network and begins processing transactions. From the earliest transactions to the most current ones, the blockchain holds all of the information about the addresses and balances of all of the participants in the system [2].

The blockchain is often regarded as Bitcoin's most important technical advance since it serves as a "trustless" proof method for all network transactions. The "miner-accountants" who maintain the "public ledger" may be trusted by users, rather than needing to develop and maintain confidence with a transaction counter-party or a third-party intermediary (like a bank). The major innovation is the use of the blockchain as the framework for a new system of trustless decentralized transactions. Every form of transaction may now be completed without the need for a third-party intermediary, thanks to the blockchain [2].

The blockchain is like a new application layer that can be added to the current internet protocol stack, providing a whole new level of economic transactions, including instant payments (in a universally usable cryptocurrency) and longer-term, more intricate financial contracts. Any money, financial contract, or asset, hard or soft, may be traded on a blockchain. In addition, the blockchain may be used to record, manage, monitor, and trade any assets, not only digital currency transactions. A blockchain is essentially a global spreadsheet for recording and transacting all types of assets owned by all parties throughout the globe, similar to a large spreadsheet. There are several ways in which the blockchain may be utilized, including intangible asset registries, inventories, and exchange; hard assets (physical property); and intangible asset exchanges (votes, ideas, reputation, intention, health data, etc.)[2].

Types of Blockchains

Three distinct blockchains may be distinguished by their participation levels and ease of use [3].

1. *Public Blockchain*: The ability to read and write is universal and does not need special permission or approval from any authority. Improved safety is achieved by using a more involved consensus technique and set of criteria. The process of mining and adding a Block is computationally intensive. There is a worldwide dispersion of computing resources.
2. *Private Blockchain*: Transaction data stored in Blockchain is accessible only to authorized nodes, and any disagreement may be settled by a single trusted node. There is a simple method to build security. When a Block is added, it is simple or requires less calculation.
3. *Federated/Consortium Blockchain*: It is a permissioned and collectively owned system in which individual control is taken away. The blockchain is managed by a network of computers rather than a single entity, and authorized nodes may access it to make changes or conduct audits. Only participating members of the consortium are able to create, verify, and evaluate transactions.

Cross-Chain Technology

Industry and academic institutions have paid a lot of attention to blockchains since the introduction of Bitcoin [4]. Numerous community efforts have resulted in important developments in the blockchain space. While Bitcoin has few functions, new blockchain implementations with expanded capabilities are constantly being developed. This makes it difficult for developers and academics to monitor the evolution of blockchains and choose the most promising solutions. Interoperability, where blockchains may talk to one another, is one way to deal with these problems [5].

This fundamental aspect of blockchains also precludes cross-chain calls to smart contracts; for example, a smart contract running on a source chain cannot call a smart contract running on a target chain. Therefore, businesses that want to collaborate through smart contracts must first settle on a common blockchain, and switching might be expensive. Cross-chain technology, which allows for communication and data sharing across blockchains, is what ultimately puts an end to these issues [5].

Regarding *T. Koens and E. Poll* [6], the following are examples of interoperability between different distributed ledger systems:

1. The possibility to use a DL with existing infrastructure. To provide two examples, Bitcoin and the centralized banking system.
2. The capacity for various DL systems to communicate with one another. Consider the differences between Bitcoin and Dogecoin (two permissionless ledgers) or Corda and Ethereum (a permissioned and permissionless ledger).
3. The ability for two smart contracts on the same blockchain to interact with one another. For instance, on the Corda ledger itself, between Corda applications.

Here the focus is on the second kind of interoperability. Based on works by *V. Buterin, H. Jin et al., A. Zamyatin et al.* [7]–[9] there are three kinds of interoperations between various DLs:

1. Notary schemes: When a trigger event occurs on ledger B, a set of participants take coordinated action on ledger A. As mentioned in Section 2.1, this coalition acts as a TTP on its own behalf. To guarantee compatibility between two or more DLs, this set of actors maintains a distinct ledger at all times [9].
2. Relay schemes: Here, a smart contract on one ledger may check the status or events of another ledger, verify them, and then act on the results. Because a replica of the other ledger is maintained in whole or in part on the ledger where the smart contracts exist, the smart contracts may access information from the other ledger. Keep in mind that two ledgers may talk to one other directly, eliminating the requirement for a middleman. There are both one-way and two-way relays available [9].
3. Hash-locking: Equally important events, such as the disclosure of the preimage of a given hash, activate operations on both ledgers. A hash-locking strategy only requires the exchange of a single hash between the two ledgers, in contrast to a relay scheme that requires a partial copy of ledger A to be maintained on ledger B. Therefore, interoperability may be achieved with hash-locking techniques with far less information transmission than with relay schemes. In this case, ledger A's cryptographic proof causes ledger B to undergo a certain transformation. The primary goal of this method is to facilitate a two-ledger atomic exchange without the need for a notary [9].

The cross-chain protocol makes it possible for data to be transferred across several blockchains and improves overall network efficiency. Users are able to interact directly with one another using the cross-chain protocol. Therefore, assets and data may be moved freely across blockchains that use the same or comparable networks [10].

Cross-chain technology is significant because it facilitates user-to-user data sharing and token trading without the need for a third party. This framework makes it possible for different blockchains to communicate with one another, increasing the efficiency, scalability, and security of the blockchain as a whole. It is crucial because it increases chain efficiency, lessens segmentation, and facilitates user communication across different blockchains. Thus, cross-chain technology has tremendous promise in facilitating blockchain interoperability, which may address a wide range of problems and free blockchain from a variety of limitations [10].

Polkadot

When it comes to interoperability, DLs need Polkadot to function as a collection of third parties. Relay chain, Polkadot's version of a blockchain, is used to record exchanges between any two DLs. While Polkadot's first release has a permissioned ledger, the intended architecture of the relay chain [11] is for it to be permissionless. Polkadot's equivalent of DLs are called parachains. A parachain bridge, enables communication with a DL. An essential part of Polkadot that is presently beyond the purview of Polkadots documentation is the network protocol, which is how the parachain bridges connect with the relay chain [11].

To manage chain upgrades, Polkadot supports a governance system in which “user” committee (made up of bonded validators) and a “technical” committee (made up of major client developers and ecosystem players) collaborate together. Major token holders are legitimate to form a super majority to augment, reparameterize, replace or dissolve this structure [11] Polkadot’s main principles are:

1. Minimal: Having as little functionality as possible.
2. Simple: If a complexity issue can be addressed in middleware layer or placed through a parachain, it should not be presented in the base protocol.
3. General: There should be no unessential limitations on parachains.
4. Robust: Providing a stable base layer alongside the decentralizing process to keep the vectors for high-reward attacks minimum.

There are four distinct functions inside the Polkadot network [11]: *Validators*, *Nominators*, *Collators*, and *Fishermen*. Collectively, validators attempt to agree on the current status of the relay chain. Every transaction is confirmed by validators that operate a complete node. Although they do not maintain a complete node, nominees may still cast votes on blocks and transmit their "DOTs" to a reliable validator. Each parachain has its own database, and it is the collator's job to store that information and generate unsealed blocks. A set of validators receives these blocks from a collator. Because of this, collators reduce the stress placed on validators during block production by performing tasks like validity and verification. It is possible to see fishermen as free-agent bounty hunters. Proof of illicit behavior is sent to them by collators or validators. Upon such evidence being shown, the collator or validator in fault will be penalized (i.e. slashed, punished for their behavior by taking away some tokens).

Polkadot is comprised of these four primary elements: *1- Relay-chain*: the shared security, consensus, and cross-chain interoperability of the Polkadot network are all the responsibility of Polkadot's core, which is also its name. Interoperability is the capability of a platform to function either as a single platform or as a reference platform. In the case of diff-diff, this capability is referred to. *2- Parachains*: A blockchain that is capable of issuing its own coins and can adapt its functionality to suit a variety of different use cases. In addition to this, it has a direct connection to the chain of relays. *3- Parathreads*: It functions in a way that is similar to parachains but on a pay-as-you-go basis. Blockchain technology does not need users to always be connected to the network, which results in significant cost savings. *4- Bridge*: Through the use of blockchain bridges, two separate blockchains that are both economically and technologically independent may connect with one another [11].

Figure 1 shows collators gather and propagate user transactions, whereas fisherman and validators propagate block candidates. In addition, it demonstrates how an account may send a transaction out of its parachain, through the relay-chain, and into another parachain, where it can be read as a transaction to another account.

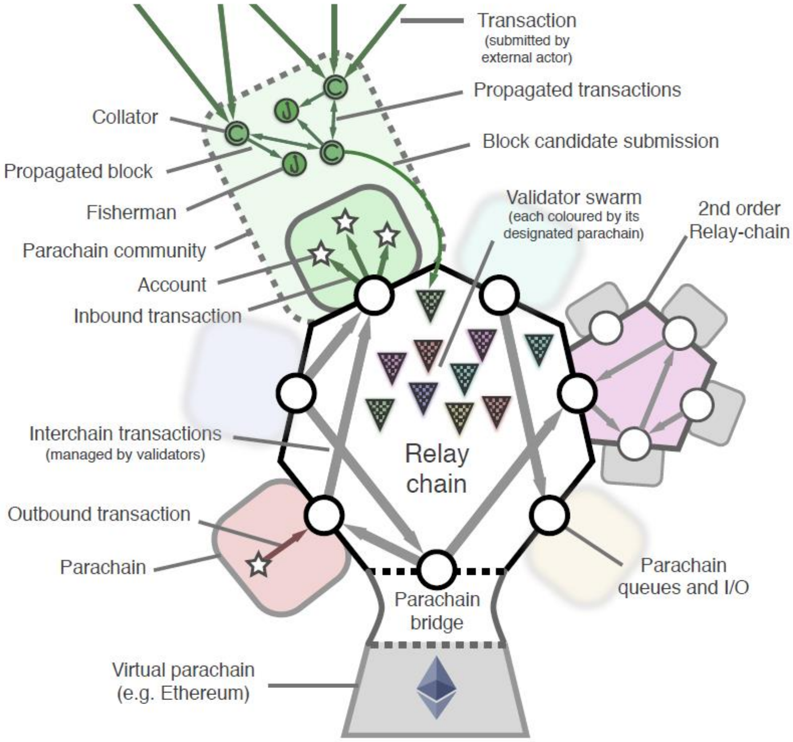


Figure 1 The schematic of the Polkadot system; borrowed from [11]

Health Applications

Regarding to Blockchain Council, there are three major categories in health industry that can be optimized with Blockchain [3].

1. *Healthcare Records Management*: Blockchains' benefits extend to the safe and secure exchange of data. When many hospitals use the same system, they are better able to work together. A hash of information including a patient's name, birth date, procedures, and medicines may be recorded on the blockchain. Wearable Internet of Things (IoT) sensors allow for automated data uploads to blockchains. Once data is encrypted on blockchains, smart contracts may be established to regulate data access. Most importantly, patients may decide who has access to their medical records, relieving healthcare professionals of the responsibility of data security. Another benefit is that EHRs can communicate with one another.
2. *Preventing Drug Counterfeiting*: The pharmaceutical industry's supply chain has become more dispersed, mirroring the trend seen in other sectors. The lack of transparency prevents the consumer or store from making informed purchases or gaining access to more reliable sources. Without a mechanism to check, hospitals may be unwittingly

giving patients access to fake medications, and consumers would have little recourse if they were given substandard goods. Producers, wholesalers, hospitals, pharmacies, and ultimately patients are the most important players in the pharmaceutical supply chain. Distributed Ledger Technology (DLT) has the potential to serve as a universal logistics network for all involved parties. The blockchain-based technology would be able to trace pharmaceuticals from the point of manufacture to the point of consumption, identify counterfeit medications, and coordinate recalls when necessary.

3. *Clinical Trials*: Due to the high degree of monitoring, control, and accuracy required to conduct clinical trials, they are also very time-consuming and costly. Falsifying or concealing information that might jeopardize the success of a clinical study is fraud. Due of the economic importance of the study's conclusions, researchers have several motivations to distort the results in their favor. Fragmented techniques of collecting data at each centre leads to numerous versions of data from external laboratories, CROs (Contract Research Organization), and other suppliers. Aggregating data from several sources may be a time-consuming manual task since hospitals in various parts of the globe gather data in different ways. Blockchain-based smart contracts can automate much of this data collection and compilation, allowing physicians to track their patients' results over longer periods of time. This is made possible by the interoperability between different blockchain platforms. The rise of wearable devices that can track steps, sleep, heart rate, etc., increases the amount of data to be stored. Any document's existence and authenticity may be verified via the use of blockchain technology. For new information to be included, it must be verified as genuine by the network as a whole. After the network has reached agreement, altering the blockchain's data would involve updating the records of the vast majority of nodes. The SHA256 hash of a document is used to keep its digital fingerprint on the blockchain and verify its validity.

Contact Tracing & Sharing Health Data

An infected person’s connections may be identified by contact tracing, which is the process of collecting more information about these individuals. Since its inception in the early stages of epidemiology, tracking contacts has been used to prevent the spread of infectious illnesses. They depended on a list of persons they had been in touch with or places they had gone recently, which was far from a thorough list. It is possible to alert persons who could be approached by letters or phone calls or emails. Because of this, the list’s completeness and correctness, as well as the process’s speed and efficiency, are constrained by the old method of tracking down contacts [12].

Due to a lack of large-scale testing and the unusually lengthy incubation period of COVID-19, authorities have struggled to determine how many people have been affected. A contact tracking procedure is the only realistic alternative. Contact tracing, according to the WHO, is a three-step technique. First, individuals who have had contact with an infected person should be identified. Then, making a list of such people and noting their specifics. Finally, it's important to have those people tested quickly. The nations now in the first and second stages of the COVID-19 epidemic may benefit from adopting the contact tracing approach.

The most debated biomedical/health care application is the use of blockchains as a core tech for Health Information Exchange (HIE), or health transactions between patients, providers, payers, as well as other related personnel [13]. Cloud-based solutions and blockchain-based solutions are examples of HIE systems that are either centralized or decentralized, respectively [14].

Many studies and projects have proposed using blockchains to store various types of healthcare–related data, such as genomics and precision medicine data, patient-related outcomes data, provider/patient directories and care plans data, clinical trial data, patient consent data, pharmaceutical supply chain data, and biomarker data, in addition to using them as patient care data ledgers [13].

Security & Privacy

1. *Byzantine Fault Tolerance*: Byzantine Fault Tolerance (BFT) is a concept in distributed computing that refers to the ability of a system to function correctly even in the presence of "Byzantine failures", which are failures caused by misbehaving or malicious nodes. In other words, a system is said to be Byzantine Fault Tolerant if it can continue to function correctly even when some of its nodes are behaving in unexpected or malicious ways. The concept was first introduced by Leslie Lamport, Robert Shostak and Marshall Pease in their 1982 paper "The Byzantine Generals Problem" [15]. BFT algorithms are designed to solve this problem by allowing nodes in a distributed system to agree on a common value, despite the presence of Byzantine failures. These algorithms typically use a combination of cryptographic techniques and consensus protocols to achieve this goal. One popular BFT algorithm is the Practical Byzantine Fault Tolerance (PBFT) algorithm, which was first introduced by Miguel Castro and Barbara Liskov in their 1999 paper "Practical Byzantine Fault Tolerance" [16].
2. *Proportional Justified Representation*: Proportional Representation (PR) is an electoral system in which the number of seats won by a political party or group of candidates is

roughly proportional to the number of votes received. This is in contrast to systems in which the number of seats won is not directly proportional to the number of votes received, such as "winner-takes-all" systems. Proportional Justified Representation (PJR) is a variation of proportional representation, which aims to ensure that the representation of different groups in society is proportional to their share of the population. This can be achieved by creating special electoral districts or by reserving a certain number of seats for specific groups, such as women, minorities or indigenous people.

3. *Maximin Support*: Maximin support is a measure of how well an electoral system supports minority groups. It is based on the idea that the system should provide the greatest possible support for the group with the smallest number of representatives, or "minority group." The maximin support is calculated by identifying the smallest number of representatives that any group receives, and then determining what proportion of the total number of representatives this represents. This proportion is known as the "minimax proportion." The maximin support is the highest possible minimax proportion that can be achieved under a given electoral system.
4. *Consensus Algorithms*: Consensus algorithms are methods used to ensure agreement on a single data value among distributed processes or systems. They are used to establish consensus in a network of nodes, where multiple nodes may have conflicting information. The consensus algorithm is responsible for determining a single, authoritative version of the data, which can then be used to update the network. Consensus algorithms are critical to the functioning of blockchain systems, as they provide a means for ensuring that all nodes in the network have a common view of the state of the blockchain. This is essential for maintaining the integrity of the blockchain, as well as ensuring that transactions are processed in a secure and efficient manner. There are several widely used consensus algorithms in blockchain, including: 1- Proof-of-Work (PoW) 2- Proof-of-Stake (PoS) 3- Delegated Proof-of-Stake (DPoS) 4- Nominated Proof-of-stake (NPoS) 5- Directed Acyclic Graph (DAG).
5. *Semi-Honest Nodes*: In the context of blockchain, a semi-honest node is one that follows the protocol correctly but may attempt to learn information that it is not supposed to know. This is in contrast to a malicious node, which actively tries to subvert the protocol and undermine the security of the network. Their semi-honest behavior can create vulnerabilities that can be exploited by attackers. For example, a semi-honest node may attempt to learn the private keys of other nodes in the network or try to manipulate the consensus process to gain an advantage. To address the challenges posed by semi-honest

nodes, researchers have proposed various approaches. One approach is to use cryptographic techniques such as zero-knowledge proofs and secure multiparty computation to ensure that sensitive information remains private even if a semi-honest node attempts to learn it. Another approach is to use reputation systems to incentivize nodes to behave honestly by rewarding good behavior and punishing bad behavior. One specific example of a technique for addressing semi-honest nodes is the use of Byzantine fault tolerance (BFT) algorithms [15]–[20].

6. *Zero-Knowledge Proof*: A zero-knowledge proof is a type of proof in which a prover can demonstrate to a verifier that they know a particular piece of information (such as a secret key or password) without revealing any other information about that piece of information. In other words, the proof provides no information beyond the fact that the prover knows the information. The article shows that zero-knowledge proofs can be used to reduce the computational complexity of interactive proof systems. Specifically, it shows that there exist interactive proof systems for certain problems that can be transformed into zero-knowledge proof systems with equivalent computational complexity. This has important implications for cryptographic protocols, as zero-knowledge proofs can be used to provide secure authentication and confidentiality without revealing sensitive information [21].

Digital contact tracing is the process of identifying individuals who have been in close proximity to a person infected with a communicable disease, such as COVID-19. This process typically involves collecting and sharing sensitive personal data, such as location data and health information, which can raise privacy concerns. One way to address these concerns is to use zero-knowledge proofs to enable privacy-preserving contact tracing. With zero-knowledge proofs, individuals can prove that they have been in contact with an infected person without revealing any other information about their movements or health status. Blockchain and Polkadot are decentralized systems that can be used to securely store and share data. By using a decentralized system, the data can be more secure and less prone to hacking or unauthorized access. Additionally, blockchain and Polkadot can enable privacy-preserving data sharing by using zero-knowledge proofs to verify the authenticity of the data without revealing the underlying information.

In conclusion, this introductory chapter has laid the foundation for exploring the potential of cross-blockchain technology in the context of an interoperable and scalable digital contact tracing system. By understanding the limitations of existing solutions and the pressing need for efficient contact tracing during public health crises, we have identified the significance of leveraging blockchain technology to overcome these challenges. The integration of multiple blockchains offers the promise of enhanced interoperability, data privacy, security, and scalability. The subsequent chapters of this thesis will delve into the technical aspects, design considerations, and implementation strategies required to develop a cross-blockchain solution for digital contact tracing. Through rigorous analysis and experimentation, we aim to contribute to the advancement of this field, ultimately paving the way for a more resilient and effective contact tracing infrastructure that can positively impact public health and societal well-being.

CHAPTER 2

Literature Review

In recent years, the digitization of healthcare data has led to a vast amount of patient information being stored electronically. While this has facilitated access to patient information, it has also presented challenges related to data sharing and privacy. Blockchain technology has emerged as a potential solution to these challenges, offering a secure and decentralized platform for sharing healthcare data. This literature review aims to provide a comprehensive overview of the current research on the use of blockchain technology in healthcare data sharing. The review will examine the benefits and drawbacks of blockchain technology, highlight key findings from relevant studies, and identify areas for future research.

Healthcare Data Sharing & Blockchain

Protecting sensitive health information and distributing the software across a variety of hospital contexts are two well-known difficulties. The main purpose of *M.A.Cyran* [22] is to answer this question whether it is possible to develop and implement a system, running on blockchain, for keeping the health records across hospitals and sharing them simply without any privacy leaks. Although blockchain provides us unique opportunities to increase the healthcare system's treatment and diagnoses efficacy, certain challenges are still in place regrading scalability and reliability before a widely-use implementation. The work by *T.-T. Kuo et al.* [13] aims to introduce and review blockchain technology to the biomedical and health care areas, including its merits, drawbacks, and most recent applications.

Also, some research teams, including MedRec, Data Lake, Healthbank, and blockchain-based data sharing networks, suggest leveraging blockchain technology to speed up secondary usage of clinical data (i.e. clinical and biomedical studies and research). ModelChain also implemented blockchain to improve the security and scalability of distributed privacy-preserving health care predictive modelling across different institutions [13].

Many studies and active initiatives are centered on transferring patient care data over blockchains in order to enhance medical record administration, including but not limited to Healthcare Data Gateways, MedVault, Fatcom, BitHealth, Gem Health Network. Several well-known firms, like

Deloitte and Accenture, are also experimenting with blockchain technology to store health care data and manage medical records. Guardtime, a startup in Estonia that provides a blockchain-based solution to safeguard 1 million health records, is another well-known example. Many studies and projects have proposed using blockchains to store various types of health care–related data, such as genomics and precision medicine data, patient-related outcomes data, provider/patient directories and care plans data, clinical trial data, patient consent data, pharmaceutical supply chain data, and biomarker data, in addition to using them as patient care data ledgers [13].

In order to meet the scalability, accessibility and security in healthcare data sharing, *M.A.Cyran* [22] proposed a blockchain-based solution alongside the cryptographic algorithms to provide integrity, security, privacy, and portability of user-owned data. The data is kept in an external storage solution, and the system's blockchain component is in charge of executing Smart Contracts. Constraints might be introduced to the system to guarantee that data files are standardized according to healthcare-related standards. They also claimed that their system is unique because of its fully containerized architecture, making it deployable across multiple hospital IT infrastructures. Their proposed system is built as a platform with a distributed microservice architecture that can scale up or down depending on deployment needs.

The first significant advantage of blockchain is decentralized administration. Distributed Database Management Systems (DDBMS) are conceptually centralized database management systems, whereas blockchain is a peer-to-peer, decentralized database management system. As a result, blockchain is appropriate for applications in which independently managed biomedical/health care parties who want to interact without relinquishing authority to a central management middleman. The immutable audit trail is the second major advantage. DDBMSs, like other database systems, provide create, read, update, and delete functions, whereas blockchain only supports creation and read functions. As a result, blockchain is suited as an immutable ledger for recording vital information. The third consideration is data provenance. On DDBMS, the system administrator can alter the ownership of digital assets, but on blockchain, the owner can only change the ownership by following the cryptographic protocols. The sources of the assets may also be traced, enhancing the re-usability of confirmed data. The fourth advantage is that it is both sturdy and available. Although DDBMS and blockchain are built on distributed technology and so do not suffer from single-point-of-failure, achieving the high level of data redundancy that blockchain achieves would be expensive for DDBMS. The latest main advantage of blockchain is increased security and privacy through the use of cryptographic algorithms. For example, the 256-bit Secure Hash Algorithm (SHA-256) is used as the cryptographic hash function in the hash-chain that the proof-of-work algorithm operates on in the Bitcoin blockchain [13].

Although transactions are cryptographically signed in Blockchain, they are transparent to everyone participating in the network. So, privacy and restricted access to the health data matters. Each piece of data, in this system, has a single user (owner) who may share it with other users or groups at various degrees of access (summary versus full data). The data sharing method is based on request and response in such a way that a cryptographic object is exposed to the receiver in such a manner that only that receiver has access to data at the given access level. In the event of access revocation, there is an additional safeguard that even a receiver's private key, along with raw blockchain transaction data, would not be sufficient to gain data access. As a file storage sector, they use the InterPlanetary File System (IPFS) separately, which is a decentralized file system. It guarantees that duplication is kept to a minimum over the whole file system network [22].

For having a robust encryption system, it would necessitate capturing the structure of submitted documents within the underlying smart contracts, such that sensitive fields are treated independently of the rest of the document. Their solution makes use of the Ethereum platform [23] for smart contract capabilities, as well as Docker containers and microservices in a distributed design. They used the Elliptic Curve Integrated Encryption System (ECIS), a hybrid of the Elliptic Curve Diffie-Hellman (ECDH) algorithm, Concatenation Key Derivation Function (KDF), and the Advanced Encryption Standard (AES-256 in Galois Counter Mode) Block Cipher for key encryption using elliptic curve primitives. All in all, The data is kept in an external storage solution, and the system's blockchain component is in charge of executing Smart Contracts. Constraints might be introduced to the system to guarantee that data files are standardized according to healthcare-related standards [22].

Blockchain in Pandemic Management

Although previous works have preciously offered some insight on the present COVID-19 scenario, they provide a short and incomplete picture of the precise issue [24]–[29]. No survey gives a thorough examination of the COVID-19 pandemic and its possible consequences. Furthermore, no previous work examines the role of future technologies such as IoT, UAVs, AI, blockchain, and 5G in managing the COVID-19 pandemic. *V. Chamola et al.* [30] offer a complete assessment of the COVID-19 pandemic, which will assist readers in acquiring a better knowledge of the current worldwide situation resulting from the COVID-19 pandemic.

One of the primary benefits of adopting blockchain-enabled apps, according to experts, is blockchain's capacity to validate continually changing data. This capability might be pretty valuable in dealing with the fast-developing COVID-19 issue. The pandemic's nature is spreading. As a result, distributed ledger technologies, such as blockchain, can be highly beneficial in dealing with this problem. Blockchain technology enables individuals and businesses worldwide to join a single linked network that allows for the secure sharing of data. The tamper-proof characteristic of blockchain makes it resistant to unauthorized modifications, and the use of consensus algorithms and smart contracts reduces the possibility of propagating fake data and fraudulent information. Blockchain-based apps can be used to digitally monitor and manage COVID-19 patients, alleviating part of the strain on hospital staff and other healthcare workers. Some of the significant ways in which blockchain technology can aid in the fight against the COVID-19 include but not limited into *Increasing Testing and Reporting Capabilities*, *Keeping Track of COVID-19 Patients' Information*, and *Managing the Implementation of a Lockdown* [30].

Proposed Systems After the COVID-19

Some of the previous main works include Singapore TraceTogether, Google/Apple Contact Tracing, UK NHS Contact Tracing, China Health Code System [31]–[34]. The first three solutions use Bluetooth technology with a high-power demand because the user is obliged to keep the device in an active broadcasting mode under this system, which consumes the user device's battery. All Bluetooth-based contact tracing systems are subject to threats such as spying, sniffing, and jamming due to the Bluetooth technology's vulnerable wireless interface. There is a significant possibility of replay attacks on the contact tracking network, resulting in widespread fear among the population. By scanning the QR code connected with the user, China Health Code System is based on relational cross-match. Because of the centralization of this system, user privacy is not protected, and the user's identity is not hidden from the authorities. On the other hand, this QR code is only scanned when passing checkpoints, saving the user's phone energy and consuming no data.

H. Xu et al. [12], introduced a system called BeepTrace. BeepTrace uses many technologies like GPS, Bluetooth, Cellular and Wi-Fi, which brings us medium power usage, high security, and privacy-preserving feature. Because of the growing amount of data supplied by users, storing enormous numbers of blockchain addresses is a daunting task for contact tracing blockchain. As a result, the use of such a system should be limited to a particular lifespan. Fortunately, contact tracing only requires a specific number of days of records, so any information older than that may be deleted. On a scale of 10,000 verified cases each day, the overall amount of storage required for notification blockchain is significantly less (a few GB compared with several hundreds of TB). Assuming that every user creates one address in 30 minutes, with N users, the number of addresses submitted to the system each second is computed as $N \times \frac{1}{30\times60}$. This amount is a true challenge for BeepTrace implementation on a large scale.

Also, the amount of raw data stored on the blockchain will be too much for the users to handle. Therefore, a compression algorithm is needed. The critical drawbacks of the proposed contact tracing approach are the high traffic generated by a vast number of address declarations due to frequent (global) geodata updates and the computational resources required for geodata matching. When it comes to implementing digital contact tracking, the limitations of technology's reach to particular groups of individuals may become a serious concern [12].

S. M. Idrees et al. [35] describe the digital contact tracking technique and the applications built so far to tackle the COVID-19 epidemic in this article. On the other side, they investigate how adopting a blockchain-based decentralized network for managing the app may give users with privacy-preserving contact tracking without sacrificing speed and efficiency.

Because users' data is gathered, tracked, tallied, and broadcast to the network, it is vital to protect user privacy and avoid identity theft. Assurances to users that only data essential to tracking COVID-19 propagation is being recorded are still inadequate. Blockchain technology may help contact tracing by enabling dispersed peer-to-peer network communication between users and app management [36].

Sharing data for decision-making processes is also problematic in a centralized network, owing to the hazards of data tampering. The blockchain-based solutions might manage this, since the network is dispersed, and the users' identities are initially hidden. Currently, decentralized applications are only accessible for limited geographical networks, which is inconvenient for individuals who travel often for business. So, a blockchain-based decentralized network can give worldwide accessibility and traceability while connecting people from all over the world. False information and rumors circulating among individuals might cause panic and should be stopped. To minimize inaccuracies or discrepancies in data, health care institutions must have trustworthy authority to review and authenticate it. So, the blockchain network is the greatest alternative, since it allows for transparent contact tracking while protecting anonymity. The transaction flow may be like this: all app users, even infected ones, will submit encrypted data to the blockchain network and do match on their own devices. Infected users may use the blockchain contact tracing software to map their contacts with the server's support. The network executes the mapping using the geographical data provided and feeds the results back to the blockchain. The servers receive geographical data from users using wireless technologies such as Wi-Fi, Bluetooth, or GPS. In addition, the government tracks all data transfers between users, path labs and servers [35].

Many nations' primary aim is to stop COVID-19 transmission from spreading in the future. As a result, contact tracing is receiving a lot of attention these days. In the battle against infectious illnesses, contact tracking is a critical pillar. COVID-19 tracking also comprises monitoring or surveillance to identify early outbreaks, safeguard the public, and effectively manage testing resources. Other challenges may include: *Test resources must be improved, Scalability issues in terms of the total number of active cases, Challenging manual contact tracing, Contact tracking and quarantine regulations are not 100 percent effective* [35].

Patients' COVID-19 symptoms, whereabouts, and health history are all recorded with utmost secrecy using blockchain technology during the epidemic. COVID-19-related data and information may now be shared more easily because to the recent emergence of several platforms that make use of this new technology. In a virus-free zone, this technology may also be used to monitor people's movements. Making the public surveillance system more effective and resilient may be achieved by combining blockchain technology with AI and Geographic Information Systems (GIS) [37].

AYUSH platform uses blockchain technology to create a transparent health record chain. When a patient transfers from one hospital to another, he/she authorizes the transfer of data. If the new hospital generates new health data, they first upload it to the IPFS file system. Its hash is added to the blockchain. The suggested approach is patient-centric, meaning the patient has control over their data. This is because the system requires a permissioned network, which would be Hyperledger Fabric [38].

Every AYUSH patient will have a public and private key established upon registration. Patients' data is encrypted using their private key. It requires decryption using their private key. So, patient decrypts the private key - which is already encoded with their passwords - and chooses which health data to disclose. Then the client decrypts the chosen data. To guarantee that only the necessary service provider gets the data, the decrypted data is encrypted again using the service provider's public key. The recipient may verify the file's integrity by recalculating the hash and comparing it to the original hash on the AYUSH blockchain network. They examine previous data after obtaining shared files from the service provider. Symptoms are posted to the blockchain after sufficient inspection. The patient's treatment records may be large, making it harder to store them on the blockchain and increasing calculation time. This may lower transaction rates. To circumvent this, the hefty records are encrypted with the patient's public key and saved on IPFS. The original field's hash is uploaded to the blockchain to verify the file's integrity if shared with another service provider. IPFS generates the hash of the encrypted file after uploading it. This helps IPFS identify files and prevents repeated uploads. The record has now been disseminated to all nodes in the network. The IPFS system now has trustworthy and immutable data. Only the patient possesses the matching private key pair, thus only he can decode the data. The new record is now part of the patient's personal health records. Similar steps may be used to distribute this data to others, if desired. To improve security, all encryption, decryption, and key creation are done at the client [38].

Blockchain & IoMT Against COVID-19

Blockchain, when used with asymmetric cryptographic techniques and digital signatures, can safeguard IoMT. Decentralization of blockchain systems also reduces the possibility of single-point failures and malicious assaults. Blockchain can protect IoMT data privacy by using privacy-preserving technologies like homomorphic obfuscation and differential privacy. So blockchain is a great IoMT carrier. Thus, deep integration of blockchain and IoMT may improve IoMT systems [39].

COVID-19 has an average incubation time of 5.5 days from infection to symptoms, and many patients are asymptomatic. To stop the spread of COVID-19, it is critical to quickly identify all social contacts that occurred during the incubation phase. Contact tracing is used to track close connections. When someone is diagnosed with COVID-19, their close contacts should be notified and given guidelines. Several mobile contact tracking apps use Bluetooth Low Energy (BLE). Using BLE, you may record nearby calls between phones, wearables, and IoT devices. The main worry with this strategy is user data security and privacy. In a centralized cloud, people lose control of their data as it is kept and processed [40].

Blockchain can handle data security and privacy issues. With blockchain, users may keep complete control of their data instead of relying on a centralized database. Patients and users may create smart contracts to limit access to patient data. Pseudo-anonymity may also preserve patients' privacy. Instead of disclosing a patient's genuine identity, the blockchain-based system might assign them a unique digital fingerprint (public key or hash) [40].

Sharing data across healthcare partners is critical in the COVID-19 pandemic. Global data sharing among foreign researchers may assist generate strong data sets that can benefit COVID-19 research. These data-sharing systems must comply with all national and international data-sharing laws. The most critical problem is patient privacy, which is preventing the widespread use of medical data exchange systems. National and international entities enforce Health Insurance Portability and Accountability Act (HIPAA) and create data access control regulations. Moreover, Internet of Medical Things (IoMT) devices may collect specific patient data such as blood oxygen levels, heart rates, and prescription dosages [40].

Blockchain's decentralized storage might substantially enhance healthcare data security and privacy. The absence of expensive middlemen in the form of centralized databases also gives patients and hospitals more control over their data. Also, blockchain may help break down conventional medical record barriers, allowing hospitals and doctors throughout the nation and perhaps globally to share data more easily. Real-time data exchange is possible with blockchain. Directly uploading IoMT data to a blockchain-based system eliminates data forgery and mutation. Transparency in data collection, storage, and sharing helps stakeholders trust one another while protecting patients' privacy [40].

CHAPTER 3

Problem Statement & Methodology

The Context & Knowledge Gap

The COVID-19 pandemic has paralyzed many lives until a vaccine has been available, which caused the so-called “new normal”. According to the World Health Organization (WHO), COVID-19 is an infectious disease. It can cause significant illness or death in anyone. Governments and health officials tried to impose rules and regulations to avoid and slow down transmission. Therefore, software engineers worldwide developed applications to trace and track patients’ movements and notify others, mainly using Bluetooth. In this way, everyone could be informed whether they come in close contact with someone who has COVID-19 and takes proper safety precautions.

Because most of the applications use technologies that can potentially reveal the user’s identity and location, researchers have debated privacy-preservation and how to improve user privacy during such pandemics. Thanks to Distributed Ledger Technology (DLT), there have been some proposed methods to develop privacy-preserving Patient Tracking Systems in the last two years. As an instance of the DLT, Blockchain is like a decentralized peer-to-peer database that maintains a record of transactions. Transactions are immutable, transparent, and anonymous in this system.

Significance

Blockchain can potentially transform the healthcare industry. Confidential and authorized data can be exchanged securely through this method. In a blockchain consortium, any healthcare organization can share medical information independently of the system it uses for its native electronic health record. We found that two major obstacles facing blockchain implementation across many healthcare systems are scalability and privacy. The Polkadot platform is presented, along with a review of its efficacy in tackling current concerns. A more scalable healthcare system is achievable in the near future using Polkadot as well as a much more privacy-preserving environment.

The purpose of this study is to investigate the solution for an effective global contact tracing system by leveraging cross-blockchain technology to achieve interoperability and scalable digital contact tracing across various public health jurisdictions. This methodology section will provide a detailed description of the research design and the proposed system model which is based on Polkadot to address the scalability and interoperability.

In a recent publication, We explored the potential applications of blockchain technology in patient tracking systems to address privacy-preserving concerns and mitigate the impact of the COVID-19 pandemic [41].   The study highlighted the potential benefits of using blockchain to enhance data security and privacy, improve transparency and traceability, and facilitate effective communication and collaboration among different stakeholders in the healthcare system. We also discussed some possible solutions for the current blockchain systems in healthcare, mainly based on Polkadot.

Approach

We offer using a framework of heterogeneous contact tracking applications using cross-blockchain technologies to increase global availability and preserve users' privacy in contrast to Bluetooth-based methods. Such capabilities may be provided by a number of cross-chain systems, such as Polkadot, Cosmos, etc.

It has been shown that existing methods of contact tracing, including some blockchain-based ones, lack the global size and efficiency required to effectively tackle the aforementioned challenges. Cross-chain technologies allow for decentralized, localized contact-tracing apps to communicate with one another. If not, they will develop into silos and attract dwindling numbers of users. One blockchain may have trouble trusting another because of fundamental differences in their underlying trust models. Most current blockchain implementations are painfully sluggish, supporting at most tens of transactions per second [42]. The difficulties in interoperability, scalability, and security that have arisen as a consequence of this separation of security functions are attempted by almost all cross-chain systems [43].

Both Polkadot and Cosmos are protocols that allow for interoperability across state machines of different types. Both protocols are founded on the theory that, in the future, there will be more than one blockchain, and these blockchains would need to communicate with one another. One open, collaborative, decentralized network (the relay chain) makes up the Polkadot system and interacts with many other chains (the parachains) that operate in parallel. Parachains are entities that offer functionality at the application level, such as cryptocurrency, contact tracking, etc., whereas the relay chain exists purely to fulfill the purpose of a heterogeneous network [43].

Chains in Cosmos are linked together using a bridge-hub mechanism. The “Cosmos Hub” is the central node, although other nodes are possible, and each node links a set of outside chains (the “zones”) throughout the system. The chain must be secured by a distributed and adequately staked collection of validators in each zone. The Inter-Blockchain Communication (IBC) protocol is used for zones to relay messages and tokens to one another. Each message is trust-bound by the recipient's confidence in the sender's security since zones do not share state, and a re-organization of one zone would not re-organize other zones. Because of the importance of each zone's independent status, its own validator community is required. Whenever one zone has to get in touch with another, it uses the IBC to transmit and receive data packets. A multi-token ledger of token balances is kept in the Hub (non-transfer messages are relayed, but their state is not stored in the Hub). A light client in each zone keeps an eye on the Hub's health, but the Hub itself is unaware of the status of the zones. Sending messages to other chains through the Hub requires Zones to utilize a deterministic finality algorithm (currently, all use Tendermint) and implement the IBC interface. Additionally, “peg zones”, which are analogous to bridged parachains, allow Cosmos to connect with external chains [43].

In Polkadot, the relay chain only communicates with the parachains over an interface, and the parachains function as untrusted external clients. The protocol is effective in establishing the externally verifiable trustworthiness of the relay chain. Polkadot is designed to be secure since it is Byzantine Fault Tolerant provided that all players are acting rationally. Assuming all interested parties have selected a validating body where at least two-thirds of the members are trustworthy. If every validator is correctly backed by the availability and validity system, then any assault against Polkadot's validity is likely to be prohibitively costly [43].

Figure 2 depicts an example implementation of the Polkadot protocol, complete with its stated structural components and functions, in a setting with six parachains, eighteen validators, and five collators per parachain. As shown in Figure 3, there are a total of 5 of these relay chain blocks in the relay chain. Parachain validators are distributed proportionally to the total number of parachains, whereas parachain collators are distributed independently. The bridge is a protocol extension that facilitates communication between Polkadot and other chains [43].

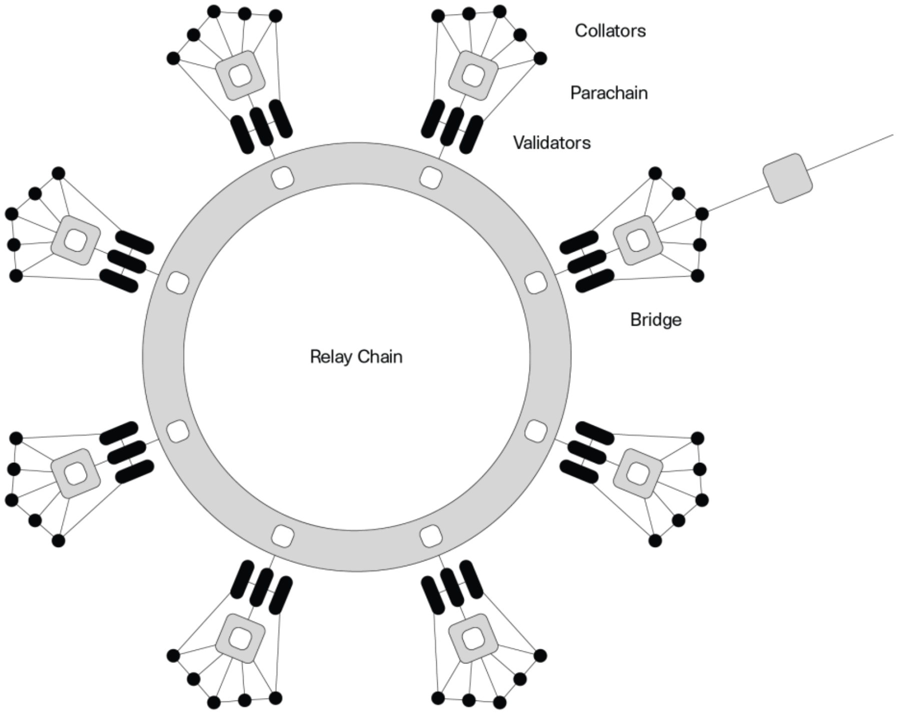


Figure 2 relay chain block securing six parachain blocks. Each parachain has five collators and three validators assigned to it (image credit: Ignasi Albero) [43]

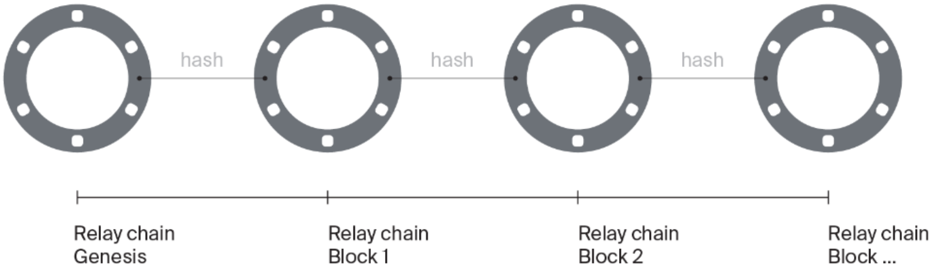


Figure 3 the relay chain with five relay chain blocks (image credit: Ignasi Albero) [43]

The hybrid consensus mechanism used by Polkadot is comprised of two smaller protocols: BABE and GRANDPA. Blind Assignment for Blockchain Extension (BABE) ensures that every slot has an author by using a verifiable random function (VRF) to allocate slots to validators, with a fallback round-robin pattern as a backup. Chains, rather than individual blocks, are up for approval in GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement).

GRANDPA may finish blocks in batches while BABE creates candidates to add to the existing chain (up to millions of blocks at a time). Separating duties has several advantages. For one, it simplifies the logistics of moving blocks between stages of manufacture and completion. BABE's linear complexity makes it simple to scale to thousands of block producers with no networking cost. While GRANDPA's complexity is quadratic, it is decreased by a factor of the latency, or the number of blocks it can complete in a single iteration.

To guarantee that no incorrect state transitions make it into the final chain, it is important that additional validators have the ability to extend the chain with unfinalized blocks. Tendermint consensus, a round-robin mechanism that delivers immediate finality, is used across Cosmos (in both the Hub and the zones). Block production and finalization are on the same route of the algorithm, meaning it generates and finalizes one block at a time. Like GRANDPA, it uses a PBFT-based algorithm and so has quadratic transport complexity, but it can only complete one block at a time [44].

The **Bridge** is a sub-protocol that lets Polkadot work with chains from outside the system. The bridge logic will consist of two essential components: a bridge relay, which comprehends the consensus of the bridged chain to the greatest extent possible, and a bank, which involves staked actors possessing tokens from the bridged chain on behalf of Polkadot. It is necessary for the bridge relay to be able to verify the consensus of the bridged chain as well as the inclusion proofs of transactions. On the one side, users on the bridging chain may use the bank to lock tokens as backing for the equivalent asset they desire to receive on Polkadot, such as PolkaETH or PolkaBTC. This can be done by using the bank's locking feature. On the other side, users have the ability to utilize the bank to convert these assets into bridging chain tokens by redeeming them. The goal of the bridge relay is to implement on a bridge parachain as much of the logic of a light or thin client of a bridged chain as is technically possible (think BTC-Relay). However, the costs of cryptography and storage on a parachain are substantially lower than those associated with an ETH smart contract. The goal is to include all block headers as well as proofs-of-inclusion of specific transactions that occurred on the bridged chain into the individual blocks that make up the bridge parachain. This alone is sufficient evidence to determine whether or not a transaction is part of a chain that is almost certainly complete. The goal of the bridge relay for Bitcoin and

ETH1.0 is to create a bridge chain that is the longest one possible and uses a vote and attestation system to settle any disputes that may arise [43].

In summary, the Polkadot network allows the interoperability of different blockchains through bridges. Bridges are specialized parachains that can communicate with external networks by replicating assets from other chains onto Polkadot as tokens. They also enable the transfer of tokens between chains and provide a way for external developers to build their own bridges to connect their chains to Polkadot. Bridges can be customized to meet specific requirements, and the Polkadot ecosystem supports multiple bridge solutions to increase flexibility and security [44].

Substrate SDK

Building a blockchain is a difficult process. Providing a trustworthy environment for programs to function necessitates mastering complex technologies like advanced encryption and distributed network connectivity. Scalability, governance, interoperability, and upgradeability are all challenging issues to tackle. Because of its intricacy, attracting new developers is difficult. To that end, the first thing to decide is what we want to construct. The Substrate is not the best option for every scenario, task, or endeavour. However, Substrate could be the appropriate solution if you wish to develop a blockchain that is: customized to a particular use case, able to connect and interact with other blockchains, customizable with predefined composable modular components, and able to grow and alter with updates over time [45].

The substrate is a Software Development Kit (SDK) particularly intended to offer all the core components a blockchain needs so we can concentrate on developing the logic that makes our chain unique and interesting. Unlike other distributed ledger systems, Substrate is Flexible, Open, Interoperable, and Future-proof [45].

Substrate owes a great deal of its success as a framework for developing important applications to Rust. Substrate has chosen Rust as its primary language because it is a fast, reliable, and safe option [45].

To achieve its speed, Rust is statically typed at build time, allowing the compiler to optimize the code for speed and the programmer to optimize for a particular compilation target. Rust is cross-platform, meaning it may be used on any device that has an operating system installed. Memory leaks are impossible in Rust since the language does not utilize a garbage collector and instead analyzes each variable and memory location used. Rust offers first-class support for compiling to WebAssembly (Wasm), making it the first language to offer this feature [45], [46].

Substrate nodes, at a high level, provide a layered environment composed of two primary components [45]:

1. A node on the network's edge responsible for tasks including peer discovery, transaction request management, peer consensus, and Remote Procedure Call (RPC) handling.
2. A runtime that implements the blockchain's state transition function and provides all of the necessary business logic to do so.

Here are the general steps that would be involved in using the Substrate SDK to develop a contact tracing parachain:

1. Setting up a development environment: We will need to set up a development environment that includes the Substrate SDK, as well as any other tools and dependencies required for building our blockchain.
2. Building the blockchain: The Substrate SDK provides a set of modular building blocks that can be used to create the custom blockchain for our contact tracing application. This would include defining the runtime modules, such as the contact registration and contact tracing modules, as well as any custom logic for the application.
3. Creating the parathread: Before creating the full-fledged parachain, we must create a parathread, which is a lighter version of a parachain and allows us to test our blockchain in the Polkadot network without needing to go through the full process of creating a parachain.
4. Testing and debugging: Once our blockchain is built, we will need to test and debug it to ensure that it is working correctly. The Substrate SDK includes tools for testing and debugging our blockchain, as well as for generating documentation and other helpful resources.
5. Submitting a proposal: Once our parathread is ready, we will need to submit a proposal to the Polkadot network for the creation of a parachain. We will need to provide detailed information about our blockchain and the benefits it will bring to the network.
6. Winning a slot auction: The Polkadot network has a limited number of slots available for new parachains, so we will need to participate in a slot auction and win a slot in order to create our parachain.

7. Bonding our DOT: Once we have won a slot, we will need to bond a certain amount of your DOT tokens as collateral to secure our parachain.
8. Launching our parachain: After bonding our DOT, we can now launch our parachain. It will be connected to the Polkadot network and be able to interoperate with other blockchains on the network.

FRAME

The FRAME development environment supplies modules (called pallets) and support libraries that may be used to construct the runtime logic of blockchain and can be customized to meet specific requirements.

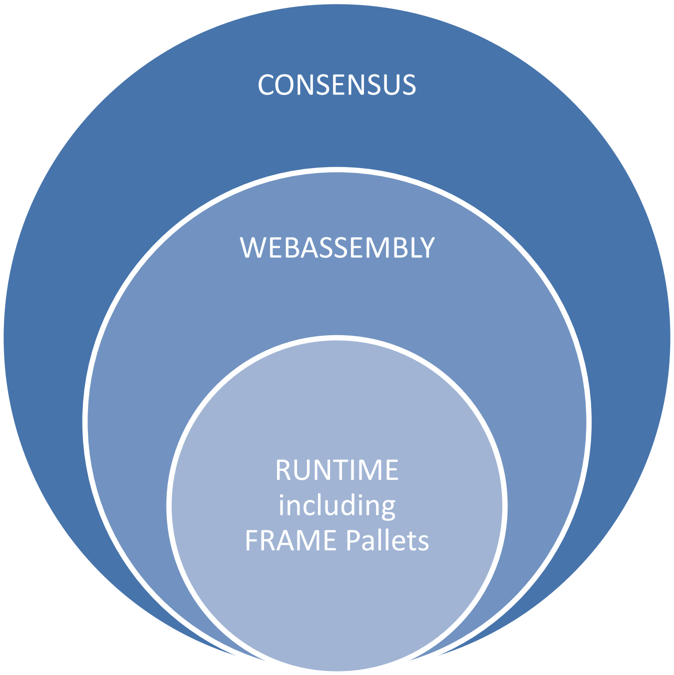


Figure 4 Anatomy of a Substrate Node

Data/Transaction Structure

A contact tracing application built on the Polkadot network would likely use transactions to record and update information about contacts between individuals.

1. Contact registration: When an individual installs the app, they would likely need to register their contact information on the network. This would involve creating a transaction that records their contact details, such as their phone number or email address, on the blockchain.

2. Contact tracing: When two individuals have a close contact, the app would likely use the Bluetooth or GPS on their devices to detect the interaction and record it as a transaction on the blockchain. This could include information such as the time and location of the contact, as well as the unique identifying information of the individuals involved.
3. Contact alerts: If an individual tests positive for COVID-19, they would likely use the app to notify their close contacts. This could involve creating a transaction that sends an alert to the individuals they have had close contact with, as well as updating their own status on the blockchain to reflect their positive test result.
4. Data sharing: To improve the effectiveness of contact tracing, it may be necessary to share data with other health authorities or other blockchain networks. Polkadot's interoperability feature allows for easy data sharing across different networks.
5. Data privacy: To ensure that sensitive personal information is protected, the app would likely use encryption and other security measures to ensure that only authorized parties can access the data.

A contact tracing application built on the Polkadot network would likely use blocks to record and store information about contacts between individuals. Each block would contain a number of transactions, each representing a specific action or event in the application. Here is an example of what the components of a block in a contact tracing app built on the Polkadot network might look like:

1. Block header: This would contain metadata about the block, such as the block number, timestamp, and hash of the previous block.
2. Transactions: Each block would contain multiple transactions, representing different events or actions within the application. For example, a transaction could be created when a user registers their contact information, or when two users have a close contact.
3. Contact Information: Each transaction would likely contain information about the individuals involved in the contact, such as their phone number, email address, and unique identifying information. It could also include the time and location of the contact.
4. Hashes: To ensure the integrity and security of the data, the block would likely contain hashes of the transactions and the contact information. These hashes would be used to verify that the data has not been tampered with.
5. Signatures: To ensure that only authorized parties can create or modify transactions, the block would likely contain digital signatures for each transaction. These signatures would be used to authenticate the identity of the parties involved.

CHAPTER 4

Experiments & Results

The goal of our research was to investigate the potential of cross-blockchain technology to develop an interoperable and scalable digital contact tracing system. We hypothesized that such a system could enhance contact tracing efforts and enable effective pandemic response. To test our hypothesis, we conducted a feasibility study using a proof-of-concept approach. We developed a simulation of a cross-blockchain contact tracing platform and proposed some possible use cases and scenarios. We analyzed the performance in terms of scalability, interoperability, and security. Our results demonstrated that our platform could effectively perform contact tracing tasks, maintain data privacy, and securely store data on multiple blockchains. The platform also showed promising scalability and interoperability, which are essential for a robust and effective contact tracing system. Overall, our findings suggest that cross-blockchain technology has the potential to provide an interoperable and scalable digital contact tracing solution for pandemics like COVID-19.

System Configuration

We used the following described system.

Operating System	Windows 11 Pro 64-bit
System Manufacturer	Dell Inc.
System Model	Vostro 14 5410
Processor	11th Gen Intel(R) Core(TM) i7-11390H @ 3.40GHz (8 CPUs), ~2.9GHz
Memory	16384MB RAM
Display Chip type	Intel(R) Iris(R) Xe Graphics Family
Display Memory	8189 MB

As a proof of concept, we used the Substrate SDK built-in palettes to resemble the digital contact tracing. We can see the block production process and other measures in Polkadot.js and a template front-end application that connects to a Substrate node back-end with minimal configuration.

We measured the system interoperability and scalability based on parameters including Transaction Per Second, Energy Consumption, and Interoperability level as follows later.

Polkadot.JS

A versatile user interface (UI) for interacting with a Polkadot or Substrate-based node is provided by the Polkadot-JS Apps. This is an effort to provide a collection of tools, utilities, and libraries that can be used to interact with the Polkadot network from within the JavaScript programming language. Although there is a lean towards developer tools, giving libraries to enable others to create tools on top of, a selection of apps are made accessible that allows for interaction with the network from a pure user viewpoint. Javascript developers are given the opportunity to query a node and interact with the Polkadot or Substrate chains thanks to the application programming interface (API) [47]. In Figure 6 and Figure 7 we can see blocks generated by nodes when the network is live and running.

Substrate Front-End Template

We will be able to interact with the Substrate-based blockchain node using a web browser interface that has been rendered by the front-end template. This interface was created using ReactJS. When we are ready to begin developing user interfaces for our own projects in the future, we may make use of this Front-end template as a starting point. Yarn and Node.js are prerequisites for the front-end template. Installing these tools should be our first step if we do not already have them [45]. In Figure 8 and Figure 9 we can see the whole front-end template generated from the functionalities and pallets used for the development.

Possible Use cases & Scenarios

Here are some example scenarios and use cases for a cross-blockchain-based contact tracing system:

Scenario 1: User uploads contact tracing data

The user installs the mobile application and enters their personal information. The user is tested positive for a contagious disease and uploads their contact tracing data to the mobile application. The mobile application encrypts the data and sends it to the blockchain network. Public health authorities access the contact tracing data on the blockchain network to identify other individuals who may have been exposed to the contagious disease and take appropriate actions.

Use Case 1: Automated Contact Tracing

This use case leverages the blockchain technology to automate the contact tracing process and reduce the time required to identify potentially infected individuals. By using the contact tracing data stored on the blockchain network, public health authorities can quickly identify other individuals who may have been exposed to the disease and take appropriate actions, such as testing and quarantining, to prevent further spread.

Scenario 2: Public Health Authority Requests Contact Tracing Data

A public health authority requests access to contact tracing data stored on the blockchain network. The blockchain network verifies the identity of the public health authority and grants access to the requested data. The public health authority uses the data to identify and contain the spread of a contagious disease.

Use Case 2: Secure Data Sharing

This use case leverages the blockchain technology to securely share contact tracing data between different stakeholders, such as public health authorities, healthcare providers, and researchers. By storing the data on the blockchain network, the system ensures that the data is tamper-proof and can only be accessed by authorized users with the proper encryption key. This helps to protect individual privacy while still allowing public health authorities and other stakeholders to use the data to identify and contain the spread of a contagious disease.

Scenario 3: User Receives Exposure Notification

A user is notified that they may have been exposed to a contagious disease. The user receives guidance on what actions they should take, such as getting tested and quarantining. Public health authorities use the contact tracing data stored on the blockchain network to identify other individuals who may have been exposed and send them exposure notifications.

Use Case 3: Early Warning System

This use case leverages the blockchain technology to provide early warning of potential outbreaks of contagious diseases. By analyzing the contact tracing data stored on the blockchain network, public health authorities can identify patterns of exposure and take proactive measures to prevent further spread. This helps to reduce the overall impact of contagious diseases and save lives.

In Figure 5 we can see the sequence diagram of mentioned scenarios and use cases.

Measuring System’s Interoperability & Scalability

Polkadot claims to offer several benefits for blockchain developers and users, such as True interoperability and Economic and transactional scalability. Polkadot enables cross-blockchain transfers of any type of data or asset, not just tokens. Connecting to Polkadot gives you the ability to interoperate with a wide variety of blockchains in the Polkadot network. Polkadot provides unprecedented economic scalability by enabling a common set of validators to secure multiple blockchains. Polkadot provides transactional scalability by spreading transactions across multiple parallel blockchains.

A comprehensive comparison between Polkadot and other cross blockchain projects for a digital contact tracing use case can be based on the following metrics:

1. ***Transactions Per Second (TPS)***: This metric indicates the throughput or performance of a blockchain system. Higher TPS means higher scalability, as it implies that the system can handle more transactions without compromising security or decentralization. For a digital contact tracing use case, higher TPS can enable faster and cheaper contact tracing transactions across multiple platforms. Polkadot can process more than 1,000 transactions per second, while Ethereum 2.0 can process up to 100,000 transactions per second. Polkadot might reach a 1,000,000 transactions per second as the network expands and parachains are added, highlighted by Gavin Wood the founder of Polkadot. Other cross blockchain projects, such as Cosmos and Near, can also achieve high TPS with their sharding and bridging solutions.
2. ***Energy Consumption***: This metric indicates the efficiency or sustainability of a blockchain system. Lower energy consumption means higher scalability, as it implies that the system can reduce its environmental impact and operational costs. For a digital contact tracing use case, lower energy consumption can enable more eco-friendly and cost-effective contact tracing transactions across multiple platforms. Polkadot consumes a small fraction of the energy used by conventional blockchains thanks to its proof-of-stake consensus mechanism. Ethereum 2.0 also claims to consume 99.95% less energy than Ethereum 1.0 with its proof-of-stake transition. Other cross blockchain projects, such as Cosmos and Near, also use proof-of-stake consensus mechanisms to reduce their energy consumption.
3. ***Interoperability Level***: This metric indicates the degree or quality of interoperability between different blockchain systems. Higher interoperability level means higher interoperability, as it implies that the systems can achieve more complex and meaningful

interactions across multiple platforms. For a digital contact tracing use case, higher interoperability level can enable more trustless and secure data and value transfer across multiple platforms. Polkadot has a high interoperability level thanks to its relay chain and parachain architecture that allows for cross-blockchain transfers of any type of data or asset. Ethereum 2.0 also aims to achieve high interoperability level with its sharded multi-chain architecture that allows for cross-shard communication. Other cross blockchain projects, such as Cosmos and Near, also have high interoperability level with their hub-and-spoke and bridge models that allow for cross-chain communication.

Based on these metrics, Polkadot seems to have a competitive edge over other cross blockchain projects for a digital contact tracing use case, as it offers high scalability and interoperability features that can enable micro validation and tokenization. However, each project has its own trade-offs and limitations, and there is no one-size-fits-all approach for digital contact tracing combined with cross blockchain technology.

Security Analysis

Polkadot's security and privacy features are some of its most important characteristics, and are essential for building a secure and reliable blockchain network. Here is a more comprehensive review of these features:

1. ***Multi-Chain Security***: Polkadot's unique architecture allows for multiple parallel chains, each with its own security features. This provides a more resilient system, as any potential security breaches or attacks are contained within a single chain, rather than affecting the entire network. Additionally, each chain can have its own customized security features, allowing for a more flexible and adaptable system.
2. ***Shared Security***: All parachains on Polkadot benefit from shared security, as they are all secured by the network's validators. This means that even smaller chains with fewer resources can benefit from the same level of security as larger chains. This shared security model helps to prevent centralization and promotes a more decentralized and democratic system.
3. ***On-Chain Governance***: Polkadot's on-chain governance system allows for community-driven decision-making, ensuring that any changes or updates to the network are made in a transparent and decentralized manner. This helps to prevent centralization and promotes a more secure and trustworthy system. The on-chain governance system also allows for

the creation of new parachains, which can be customized to meet specific security and privacy requirements.

4. ***Privacy***: Polkadot's privacy features include the ability to create private or confidential transactions, as well as the option to keep certain data hidden from the public. This can be useful for sensitive financial or personal information that needs to be kept confidential. Polkadot's privacy features are based on zero-knowledge proofs, which allow for secure and private transactions without revealing any underlying data.
5. ***Interoperability***: Polkadot's ability to connect with other blockchain networks via its cross-chain messaging system (XCMP) allows for the secure and private transfer of assets and data between different networks. This interoperability feature is essential for building a robust and scalable blockchain ecosystem, as it allows for the seamless transfer of data and assets across different networks.

Oyente is an open-source tool for analyzing and auditing smart contracts written in the Solidity programming language used for Ethereum blockchain. It is designed to automatically detect security vulnerabilities in smart contracts that may lead to unexpected behavior or allow malicious actors to exploit them. Oyente uses several techniques to analyze the code, including symbolic execution, taint analysis, and control flow checking. These techniques allow Oyente to identify potential issues such as reentrancy attacks, integer overflows, and other vulnerabilities that may arise from incorrect or incomplete programming. The tool was initially developed by a team of researchers at the National University of Singapore and has since been maintained by the open-source community. Oyente has been widely used by developers and auditors to detect potential security issues in their smart contracts before deployment, reducing the risk of contract failure or exploitation [48].

Oyente is specifically designed for analyzing and auditing smart contracts written in the Solidity programming language, which is used by the Ethereum blockchain. Polkadot, on the other hand, is a multi-chain network that supports multiple programming languages for smart contract development, including Solidity, Ink!, and Rust. Since Oyente is tailored for Solidity, it may not be directly applicable for auditing smart contracts written in other languages supported by Polkadot. However, the underlying principles of smart contract security and the techniques used by Oyente, such as symbolic execution and taint analysis, may still be relevant for auditing smart contracts in other languages.Therefore, while Oyente may not be directly applicable for Polkadot, its methodology and techniques can still be useful in the broader context of smart contract auditing and security.

While there are several tools available for auditing smart contracts, there is no comprehensive tool that meets all the requirements of a smart contract auditing tool for Polkadot. Therefore, further research and development are required to address the limitations and gaps identified in the current landscape of smart contract auditing tools for Polkadot.

Comparison & Discussion

Compared to other blockchain-based contact tracing apps, a Polkadot-based app could potentially provide the following advantages:

1. ***Scalability***: Polkadot's unique architecture allows it to scale more efficiently compared to other blockchains. This could be beneficial for a contact tracing app that requires a high level of scalability to keep up with the speed of transmission.
2. ***True Interoperability***: As mentioned earlier, Polkadot's interoperability feature could enable a contact tracing app to connect and communicate with other blockchain-based contact tracing apps. This could help create a more comprehensive and efficient contact tracing system.
3. ***Customizability***: Polkadot allows for customizable blockchain design, which could allow for the creation of a contact tracing app that fits the specific needs of a particular jurisdiction or demographic.

Here's a qualitative comparison between a Polkadot-based contact tracing app and some other existing blockchain-based contact tracing apps, focusing on similarities and potential differences.

Features	AYUSH	BeepTrace	China Health Code	Singapore TraceTogether & UK NHS App	Google/Apple	Polkadot-based proposed method
Blockchain	✓	✓	✗	✗	✗	✓
Security/Privacy	✓	✓	✗	✗	✗	✓
Decentralization	✓	✓	✗	✗	✗	✓
Interoperability	✗	✗	✗	✗	✗	✓
Scalability	✗	✗	✗	✗	✗	✓
Complexity	✗	✗	✗	✗	✗	✓
Customizability	✗	✗	✗	✗	✗	✓

Table 1 Comparison between the proposed method and existing ones

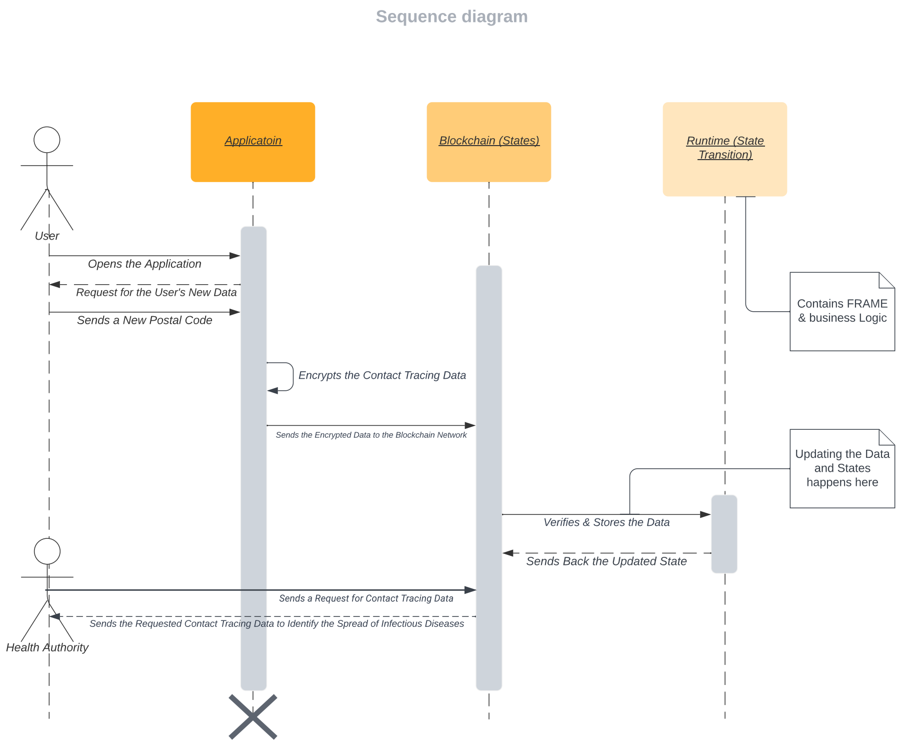
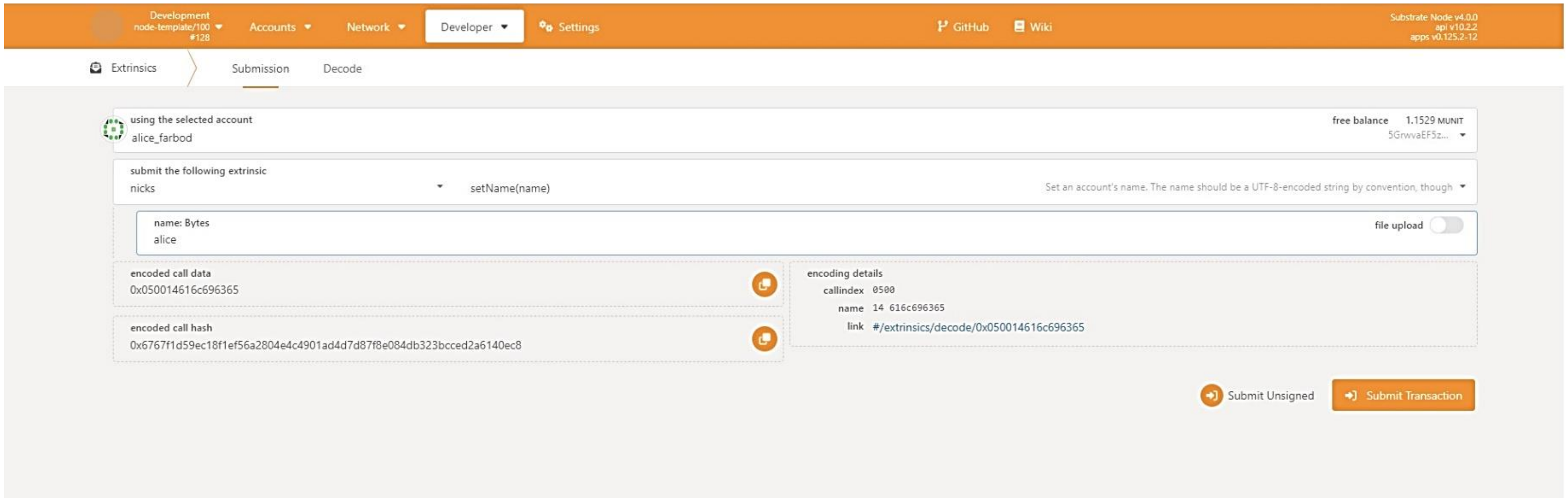

Sequence diagram
Applicatoin
Blockchain (States)
Runtime (State Transition)
User
Opens the Application
Request for the User's New Data
Sends a New Postal Code
Contains FRAME & business Logic
Encrypts the Contact Tracing Data
Sends the Encrypted Data to the Blockchain Network
Updating the Data and States happens here
Verifies & Stores the Data
Sends Back the Updated State
Sends a Request for Contact Tracing Data
Sends the Requested Contact Tracing Data to Identify the Spread of Infectious Diseases
Health Authority

Figure 5 Sequence Diagram of Possible Scenarios



using the selected account: alice_farbod

free balance 1.1529 MUNIT

5GrwvaEF5z...

submit the following extrinsic: nicks setName(name)

Set an account's name. The name should be a UTF-8-encoded string by convention, though

name: Bytes: alice

file upload

encoded call data: 0x050014616c696365

encoded call hash: 0x6767f1d59ec18f1ef56a2804e4c4901ad4d7d87f8e084db323bcced2a6140ec8

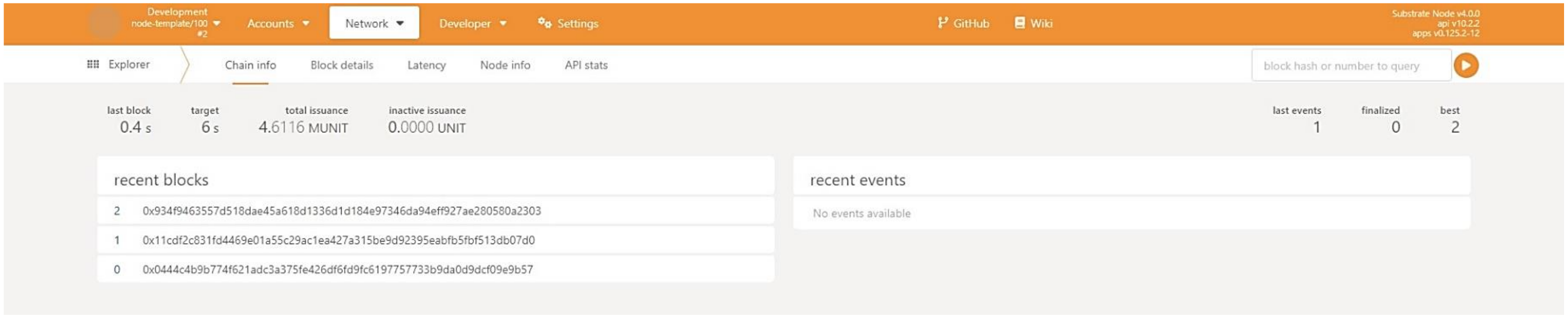
encoding details

callindex 0500

name 14 616c696365

link #/extrinsics/decode/0x050014616c696365

Figure 6 Polkadot.js Extrinsic Dashboard



last block 0.4 s
target 6 s
total issuance 4.6116 MUNIT
inactive issuance 0.0000 UNIT
last events 1
finalized 0
best 2

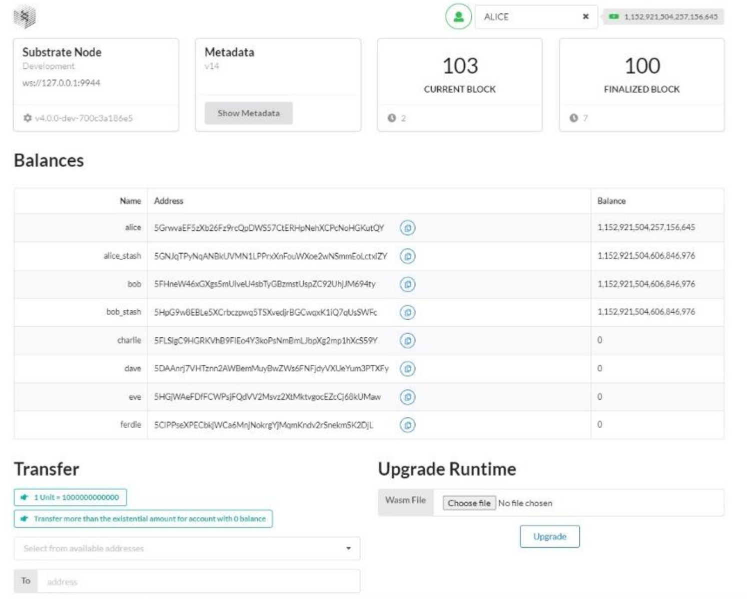
recent blocks

```
2    0x934f9463557d518dae45a618d1336d1d184e97346da94eff927ae280580a2303
1    0x11cdf2c831fd4469e01a55c29ac1ea427a315be9d92395eabfb5fbf513db07d0
0    0x0444c4b9b774f621adc3a375fe426df6fd9fc6197757733b9da0d9dcf09e9b57
```

recent events

No events available

Figure 7 Blocks and Network status in Polkadot.js



ALICE ✖ 1,152,921,504,257,156,645

Substrate Node
Development
ws://127.0.0.1:9944
v4.0.0-dev-700c3a186e5

Metadata
v14
Show Metadata

103
CURRENT BLOCK
2

100
FINALIZED BLOCK
7

Balances

Name	Address	Balance
alice	5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY	1,152,921,504,257,156,645
alice_stash	5GNJqTPyNqANBkUVMN1LPPrxXnFouWXoe2wNSmmEoLctxiZY	1,152,921,504,606,846,976
bob	5FHneW46xGXgs5mUiveU4sbTyGBzmstUspZC92UhjJM694ty	1,152,921,504,606,846,976
bob_stash	5HpG9w8EBLe5XCrbczpwq5TSXvedjrBGCwqxK1iQ7qUsSWFc	1,152,921,504,606,846,976
charlie	5FLSigC9HGRKVhB9FiEo4Y3koPsNmBmLJbpXg2mp1hXcS59Y	0
dave	5DAAnrj7VHTznn2AWBemMuyBwZWs6FNFjdyVXUeYum3PTXFy	0
eve	5HGjWAeFDfFCWPsjFQdVV2Msvz2XtMktvgocEZcCj68kUMaw	0
ferdie	5CiPPseXPECbkjWCa6MnjNokrgYjMqmKndv2rSnekmSK2DjL	0

Transfer

1 Unit = 1000000000000

Transfer more than the existential amount for account with 0 balance

Select from available addresses

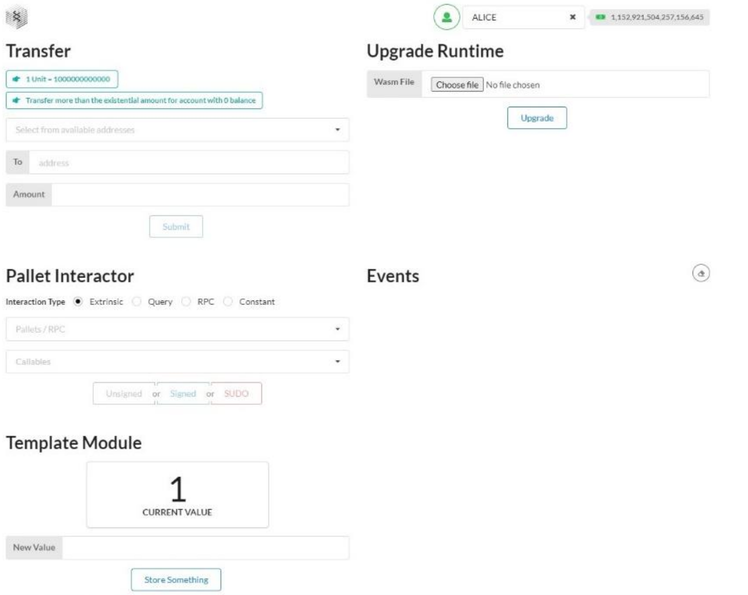
To address

Upgrade Runtime

Wasm File Choose file No file chosen

Upgrade

Figure 8 Template Front-end (1)



ALICE ✖ 1,152,921,504,257,156,645

Transfer

1 Unit = 1000000000000

Transfer more than the existential amount for account with 0 balance

Select from available addresses

To address

Amount

Submit

Upgrade Runtime

Wasm File Choose file No file chosen

Upgrade

Pallet Interactor

Interaction Type ● Extrinsic ○ Query ○ RPC ○ Constant

Pallets / RPC

Callables

Unsigned or Signed or SUDO

Events

Template Module

1
CURRENT VALUE

New Value

Store Something

Figure 9 Template Front-end (2)

CHAPTER 5

Conclusion & Future Work

In this thesis, we proposed a cross-chain technology-based digital contact tracing system using Polkadot, which addresses the challenges faced by existing contact tracing solutions. The proposed system leverages the interoperable and scalable features of blockchain networks, ensuring data privacy and security, scalability, and interoperability across different blockchain networks.

We conducted a comprehensive literature review, highlighting the potential of blockchain technology in healthcare data sharing, pandemic management, and contact tracing. We also identified the limitations of existing solutions and the knowledge gap that our proposed system can address.

Using Substrate SDK and FRAME, we designed and implemented a proof-of-concept prototype, showcasing the system's interoperability, scalability, and security features. Our experiments and results demonstrated the system's ability to handle a large volume of data efficiently, making it a viable solution for large-scale digital contact tracing.

Limitations & Challenges

Limitations and challenges of the proposed system were identified, including the need for further optimization and user-friendly interfaces to improve usability. There are some limitations to using Polkadot to develop a contact tracing application:

1. Scalability: While Polkadot aims to provide scalability by allowing interoperability between different chains, it is still a relatively new platform and has not yet been fully tested in a production environment. It may not be able to handle the large amounts of data and transactions that a contact tracing application would require.
2. Privacy Concerns: Contact tracing applications typically require the collection and storage of sensitive personal information, such as location data and contact details. The use of blockchain technology alone may not be sufficient to ensure the privacy and security of this data, especially when it comes to interoperability with other chains that may have different privacy standards.

3. Regulation: Contact tracing applications are subject to a variety of regulations and laws, such as data protection and privacy laws. It is important to ensure that the application is compliant with all relevant regulations, which may be difficult when working with a decentralized platform like Polkadot.
4. Adoption: Contact tracing applications rely on a large number of users to be effective. It can be a challenge to achieve a critical mass of users for a new platform like Polkadot, especially when compared to more established platforms that already have a user base.
5. Complexity: Developing a contact tracing application on Polkadot would require a deep understanding of the platform and its unique features. The process can be complex and time-consuming, especially for developers who are not familiar with the platform.
6. Substrate Pallets Limitations: There are a few potential limitations to consider when using these pallets including: Customization, Complexity, Compatibility, and Documentation. Developers may need to build custom pallets or modify existing ones to achieve the desired functionality. While Substrate pallets are designed to work well together, there may be compatibility issues when integrating pallets from different sources or with other blockchain systems.

Developing a digital contact tracing blockchain-based app using the Substrate framework is a complex and challenging task that typically requires a team of experienced developers with expertise in blockchain technology, software development, cryptography, and data privacy. It is not recommended for a single person to attempt to develop such an application alone as it requires a significant amount of time, resources, and expertise.

Furthermore, developing a blockchain-based application involves multiple stages, including planning, designing, coding, testing, deployment, and maintenance. Each stage requires different skills and knowledge, and a team of developers can bring diverse perspectives and expertise to each stage, increasing the likelihood of success.

Therefore, it's essential to have a team of skilled professionals to work on developing a digital contact tracing blockchain-based app using the Substrate framework to ensure the app's success and reliability.

In order to provide a consistent, open, and permissionless method of allocating parachain resources, auctions are used. All things considered, anybody who wants a parachain space has to enter an auction and bid in DOTs - Polkadot's native token. The highest bidder is awarded the time slot and its bid becomes a refundable deposit when the allotted time has passed. Therefore, the slot rental fee is equivalent to the opportunity cost of locking up this money. The parachain's voting stake in Polkadot's administration is likewise cemented by this DOT deposit. This design aims to minimize griefing attempts by parties that boost the value of the winning bid without intending to win themselves, to provide less financed projects with a chance of winning a slot, and to secure the decentralized character of Polkadot [43].

Since contact tracing methods need to be implemented soon after an epidemic strikes, we see this as a possible shortcoming of our effort. In such situations, parachain slot allocation should be easy and almost certain. Participating in the Polkadot auction process can be expensive, as bidders must stake DOT tokens as collateral during the auction. The number of parachain slots available on the Polkadot network is limited, and the auction process can be highly competitive, making it difficult to secure a slot for our project. This issue may be overcome with global and governmental efforts to bid enough DOTs for a guaranteed parachain space. To be more specific, the World Health Organization (WHO) could provide funding support to developers to help address the cost of participation in the Polkadot auction process. This could include grants, loans, or other forms of financial support, which could help to reduce the financial barriers to entry and encourage more participation from smaller projects or teams. The WHO could provide technical support to developers in addressing the limitations of the Substrate pallets, including identifying and addressing bugs, improving functionality, and integrating new features. The WHO could also help developers to design and implement the app in a way that is compatible with the Polkadot network and the wider blockchain ecosystem.

The WHO could help to establish standards and best practices for digital contact tracing blockchain-based apps, including guidelines for data privacy and security, interoperability, and community engagement. By setting clear standards and guidelines, the WHO could help to promote consistency and quality across different apps and projects. The WHO could play a key role in engaging with stakeholders such as public health officials, healthcare workers, and the general public to promote awareness and adoption of digital contact tracing blockchain-based apps. This could include developing public awareness campaigns, providing education and training materials, and engaging with local communities to build trust and understanding of the apps. The WHO could provide policy and regulatory support to developers to help ensure that digital contact tracing blockchain-based apps are compliant with relevant regulations and standards. This could include working with national and international regulatory bodies to develop clear guidelines and requirements for the apps, and providing guidance on issues such as data privacy and security, liability, and accountability.

Future Research Directions

Future work includes the implementation of the proposed system in real-world settings by full implementation of the “contact_tracing” pallet and conducting a thorough evaluation of its performance and scalability. Additionally, the system can be further optimized by integrating machine learning techniques to enhance the accuracy and efficiency of contact tracing. Furthermore, the system's usability can be improved by designing user-friendly interfaces that facilitate user engagement and adoption. Other than the health industry, digital contact tracing using cross-blockchain technologies can be used in several other applications, including:

1. Supply Chain Management: Contact tracing can be used to trace the origins of products and raw materials and to track the movement of goods throughout the supply chain. This can be used to improve efficiency and transparency, as well as to ensure compliance with regulations and standards.
2. Environmental Monitoring: Contact tracing can be used to track the movement of wildlife and other animals, as well as to monitor the spread of invasive species and pollutants.
3. Food Safety: Contact tracing can be used to track the origins of food products and to monitor their movement throughout the food supply chain. This can be used to improve food safety and to identify the source of outbreaks of food-borne illnesses.
4. Logistics and Transportation: Contact tracing can be used to track the movement of vehicles and cargo and to monitor the performance of logistics and transportation systems.
5. Fraud Detection: Contact tracing can be used to track the movement of individuals and assets and to identify patterns of suspicious activity. This can be used to detect and prevent fraud in various industries such as banking and finance, insurance, and telecommunications.
6. Cybersecurity: Contact tracing can be used to track the movement of data and to identify patterns of suspicious activity. This can be used to detect and prevent cyber-attacks and data breaches.
7. Social Media: Contact tracing can be used to track the spread of information and disinformation on social media platforms and to identify sources of misinformation.
8. Human Resource Management: Contact tracing can be used to track the movement of employees and to monitor attendance and performance.

In conclusion, the proposed cross-chain technology-based digital contact tracing system is a promising solution for addressing the challenges of existing contact tracing solutions. Its scalability, interoperability, and security features make it a viable solution for large-scale digital contact tracing. We hope that our work will pave the way for further research and development in this field, ultimately contributing to better public health management and pandemic response efforts.

REFERENCES

[1] A. Khatoon, “Use of blockchain technology to curb Novel Coronavirus Disease (COVID-19) transmission,” *Available SSRN 3584226*, 2020.

[2] M. Swan, *Blockchain: Blueprint for a new economy*. O’Reilly Media, Inc., 2015.

[3] “Certified Blockchain & Healthcare Professional | Blockchain Council,” 2021. https://www.blockchain-council.org/certifications/certified-blockchain-healthcare-professional/

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Decentralized Bus. Rev.*, p. 9, 2008.

[5] M. Nissl, E. Sallinger, S. Schulte, and M. Borkowski, “Towards Cross-Blockchain Smart Contracts.” arXiv, Jun. 28, 2021.

[6] T. Koens and E. Poll, “Assessing interoperability solutions for distributed ledgers,” *Pervasive Mob. Comput.*, vol. 59, p. 101079, Oct. 2019, doi: 10.1016/j.pmcj.2019.101079.

[7] V. Buterin, “Chain Interoperability,” *R3 Res. Pap.*, vol. 9, p. 25, 2016.

[8] H. Jin, X. Dai, and J. Xiao, “Towards a Novel Architecture for Enabling Interoperability amongst Multiple Blockchains,” in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2018, pp. 1203–1211. doi: 10.1109/ICDCS.2018.00120.

[9] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, “XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets,” in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019, pp. 193–210. doi: 10.1109/SP.2019.00085.

[10] “Blockchain Interoperability - Understanding Cross-Chain Technology,” Mar. 01, 2022. https://www.blockchain-council.org/blockchain/blockchain-interoperability/

[11] G. Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” *White Pap.*, vol. 21, pp. 2327--4662, 2016.

[12] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, “BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond,” *IEEE Internet Things J.*, 2020.

[13] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *J. Am. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

[14] Y. Alabdulkarim, A. Alameer, M. Almukaynizi, and A. Almaslukh, “SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations,” *Appl. Sci.*, vol. 11, no. 18, p. 8767, 2021, doi: http://dx.doi.org/10.3390/app11188767.

[15] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Trans. Program. Lang. Syst.*, pp. 382–401, Jul. 1982.

[16] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” *OsDI*, vol. 99, pp. 173–186, 1999.

[17] Y. Lindell, “Secure Multiparty Computation for Privacy Preserving Data Mining,” in *Encyclopedia of Data Warehousing and Mining*, IGI global, 2005, pp. 1005–1009.

[18] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, “A Survey on Zero-Knowledge Proof in Blockchain,” *IEEE Netw.*, vol. 35, no. 4, pp. 198–205, Jul. 2021, doi: 10.1109/MNET.011.2000473.

[19] C. Cachin and M. Vukolić, “Blockchain Consensus Protocols in the Wild,” in *31 International Symposium on Distributed Computing*, Jul. 2017.

[20] E. Buchman, “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains,” Master of Applied Science Thesis, University of Guelph, Guelph, 2016.

[21] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof-systems,” in *Proceedings of the seventeenth annual ACM symposium on Theory of computing - STOC ’85*, Providence, Rhode Island, United States: ACM Press, 1985, pp. 291–304. doi: 10.1145/22145.22178.

[22] M. A. Cyran, “Blockchain as a Foundation for Sharing Healthcare Data,” *Blockchain Healthc. Today*, Mar. 2018, doi: 10.30953/bhty.v1.13.

[23] D. G. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger”.

[24] L. Fang, G. Karakiulakis, and M. Roth, “Are patients with hypertension and diabetes mellitus at increased risk for COVID-19 infection?,” *Lancet Respir. Med.*, vol. 8, no. 4, p. e21, 2020, doi: 10.1016/S2213-2600(20)30116-8.

[25] S. H. Wong, R. N. Lui, and J. J. Sung, “Covid-19 and the digestive system,” *J. Gastroenterol. Hepatol.*, vol. 35, no. 5, pp. 744–748, 2020, doi: 10.1111/jgh.15047.

[26] R. Baldwin and E. Tomiura, “Thinking ahead about the trade impact of COVID-19,” *Lond. UK*, vol. 59, pp. 59–71, 2020.

[27] The Novel Coronavirus Pneumonia Emergency Response Epidemiology Team, “The Epidemiological Characteristics of an Outbreak of 2019 Novel Coronavirus Diseases (COVID-19) — China, 2020,” *China CDC Wkly.*, vol. 2, no. 8, pp. 113–122, Feb. 2020.

[28] H. Chen *et al.*, “Clinical characteristics and intrauterine vertical transmission potential of COVID-19 infection in nine pregnant women: a retrospective review of medical records,” *The Lancet*, vol. 395, no. 10226, pp. 809–815, Mar. 2020, doi: 10.1016/S0140-6736(20)30360-3.

[29] D. Wang *et al.*, “Clinical Characteristics of 138 Hospitalized Patients With 2019 Novel Coronavirus–Infected Pneumonia in Wuhan, China,” *JAMA*, vol. 323, no. 11, pp. 1061–1069, Mar. 2020, doi: 10.1001/jama.2020.1585.

[30] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, “A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact,” *IEEE Access*, vol. 8, pp. 90225–90265, 2020, doi: 10.1109/ACCESS.2020.2992341.

[31] J. Bay *et al.*, “BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders,” *Gov. Technol. Agency-Singap. Tech Rep*, vol. 18, p. 1, 2020.

[32] Apple, “Privacy-Preserving Contact Tracing - Apple and Google,” *Apple*. https://www.apple.com/covid19/contacttracing

[33] I. Levy, “The security behind the nhs contact tracing app,” *National Cyber Security Centre*, vol. 4, 2020.

[34] P. Mozur, R. Zhong, and A. Krolik, “In coronavirus fight, China gives citizens a color code, with red flags,” *The New York Times*, vol. 1, 2020.

[35] S. M. Idrees, M. Nowostawski, and R. Jameel, “Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions,” *JMIR Med. Inform.*, vol. 9, no. 2, p. e25245, Feb. 2021, doi: 10.2196/25245.

[36] P. Durneva, K. Cousins, and M. Chen, “The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review,” *J. Med. Internet Res.*, vol. 22, no. 7, p. e18619, Jul. 2020, doi: http://dx.doi.org/10.2196/18619.

[37] A. Sharma, S. Bahl, A. K. Bagha, M. Javaid, D. K. Shukla, and A. Haleem, “Blockchain technology and its applications to combat COVID-19 pandemic,” *Res. Biomed. Eng.*, Oct. 2020, doi: 10.1007/s42600-020-00106-3.

[38] A. V. Aswin, K. Y. Basil, V. P. Viswan, B. Reji, and B. Kuriakose, “Design of AYUSH: A Blockchain-Based Health Record Management System,” in *Inventive Communication and Computational Technologies*, Singapore: Springer, 2020, pp. 665–672. doi: 10.1007/978-981-15-0146-3_62.

[39] H.-N. Dai, M. Imran, and N. Haider, “Blockchain-enabled Internet of Medical Things to Combat COVID-19,” *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 52–57, 2020.

[40] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, “The role of blockchain to fight against COVID-19,” *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 85–96, 2020.

[41] F. Behnaminia and S. Samet, “Blockchain Technology Applications in Patient Tracking Systems Regarding Privacy-Preserving Concerns and COVID-19 Pandemic,” *World Acad. Sci. Eng. Technol.*, vol. 17, no. 2, pp. 144–156, Feb. 2023.

[42] K. Croman *et al.*, “On Scaling Decentralized Blockchains,” in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, pp. 106–125. doi: 10.1007/978-3-662-53357-4_8.

[43] J. Burdges *et al.*, “Overview of Polkadot and its Design Considerations.” arXiv, May 29, 2020.

[44] Polkadot, “The hub for those interested in learning, building, or running a node on Polkadot. · Polkadot Wiki,” *Polkadot Wiki*, 2022. https://wiki.polkadot.network/

[45] Substrate, “Why Substrate? | Substrate_ Docs.” https://docs.substrate.io

[46] “The Rust Programming Language - The Rust Programming Language.” https://doc.rust-lang.org/book/title-page.html

[47] “Overview | polkadot{.js}.” https://polkadot.js.org/docs/

[48] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, in CCS ’16. New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 254–269. doi: 10.1145/2976749.2978309.

APPENDICES

Appendix A – Substrate Pallets

The compiler's configuration file must be updated to utilize a new pallet.

Cargo.toml defines Rust program configuration variables and dependencies. The Cargo.toml file handles two crucial pieces of information since the Substrate runtime compiles to both a native platform binary with standard library Rust functions and a WebAssembly (Wasm) binary without the standard Rust library. In other words they include: 1. The runtime dependencies to import, including location and version. 2. Pallet features to allow for native Rust binary compilation. Enabling the standard (std) feature set from each pallet compiles the runtime to include functions, types, and primitives that would otherwise be missing when building the WebAssembly binary.

To add the dependencies to the runtime we:

1. Enter the node template root directory in a terminal shell.
2. Open runtime/Cargo.toml in an editor.
3. See how other pallets are imported in [dependencies] section.
4. Copy a pallet dependency description and change the pallet name with the desired pallet to make it accessible to the node template runtime.
5. Add the pallet features to the list of features in the Cargo file.
6. Run this command to verify new dependencies:

```
cargo check -p node-template-runtime --release
```

We used and added the following substrate pallets among the existing ones to build the prototype close enough to what we proposed.

1. The Aura module extends Aura consensus by managing offline reporting.
2. The Balances module provides functionality for handling accounts and balances. The Balances module provides functions for:
    a. Getting and setting free balances.

b. Retrieving total, reserved and unreserved balances.
c. Repatriating a reserved balance to a beneficiary account that exists.
d. Transferring a balance between accounts (when not reserved).
e. Slashing an account balance.
f. Account creation and removal.
g. Managing total issuance.
h. Setting and managing locks.

3. GRANDPA Consensus module for runtime.
4. The Sudo module allows for a single account (called the "sudo key") to execute dispatchable functions that require a Root call or designate a new account to replace them as the sudo key. Only one account can be the sudo key at a time.
5. The Timestamp module provides functionality to get and set the on-chain time.
6. The Transaction Payment module provides the basic logic needed to pay the absolute minimum amount needed for a transaction to be included.

```
[dependencies]

pallet-aura = { version = "4.0.0-dev", default-features = false,
git = "https://github.com/paritytech/substrate.git", branch =
"polkadot-v0.9.40" }

pallet-balances = { version = "4.0.0-dev", default-features =
false, git = "https://github.com/paritytech/substrate.git",
branch = "polkadot-v0.9.40" }

pallet-grandpa = { version = "4.0.0-dev", default-features =
false, git = "https://github.com/paritytech/substrate.git",
branch = "polkadot-v0.9.40" }

pallet-sudo = { version = "4.0.0-dev", default-features = false,
git = "https://github.com/paritytech/substrate.git", branch =
"polkadot-v0.9.40" }

pallet-timestamp = { version = "4.0.0-dev", default-features =
false, git = "https://github.com/paritytech/substrate.git",
branch = "polkadot-v0.9.40" }
```

```
pallet-transaction-payment = { version = "4.0.0-dev", default-features = false, git = "https://github.com/paritytech/substrate.git", branch = "polkadot-v0.9.40" }
```

```
[features]
default = ["std"]
std = [
    "pallet-aura/std",
    "pallet-balances/std",
    "pallet-grandpa/std",
    "pallet-sudo/std",
    "pallet-template/std",
    "pallet-timestamp/std",
    "pallet-transaction-payment-rpc-runtime-api/std",
    "pallet-transaction-payment/std",
]
```

Every pallet has the Rust trait Config. The Config trait specifies the parameters and types the pallet requires to work. Config implements most pallet-specific code. The pallet's Rust documentation or source code will tell us what to implement. We can see the following example for our pallets.

```
impl pallet_aura::Config for Runtime {
   type AuthorityId = AuraId;
   type DisabledValidators = ();
   type MaxAuthorities = ConstU32<32>;
}

impl pallet_grandpa::Config for Runtime {
   type RuntimeEvent = RuntimeEvent;

   type WeightInfo = ();
```

```
    type MaxAuthorities = ConstU32<32>;
    type MaxSetIdSessionEntries = ConstU64<0>;

    type KeyOwnerProof = sp_core::Void;
    type EquivocationReportSystem = ();
}

impl pallet_timestamp::Config for Runtime {
    /// A timestamp: milliseconds since the unix epoch.
    type Moment = u64;
    type OnTimestampSet = Aura;
    type MinimumPeriod = ConstU64<{ SLOT_DURATION / 2 }>;
    type WeightInfo = ();
}
impl pallet_balances::Config for Runtime {
    type MaxLocks = ConstU32<50>;
    type MaxReserves = ();
    type ReserveIdentifier = [u8; 8];
    /// The type for recording an account's balance.
    type Balance = Balance;
    /// The ubiquitous event type.
    type RuntimeEvent = RuntimeEvent;
    type DustRemoval = ();
    type ExistentialDeposit = ConstU128<EXISTENTIAL_DEPOSIT>;
    type AccountStore = System;
    type WeightInfo =
pallet_balances::weights::SubstrateWeight<Runtime>;
}

parameter_types! {
    pub FeeMultiplier: Multiplier = Multiplier::one();
}

impl pallet_transaction_payment::Config for Runtime {
    type RuntimeEvent = RuntimeEvent;
    type OnChargeTransaction = CurrencyAdapter<Balances, ()>;
    type OperationalFeeMultiplier = ConstU8<5>;
    type WeightToFee = IdentityFee<Balance>;
    type LengthToFee = IdentityFee<Balance>;
    type FeeMultiplierUpdate = ConstFeeMultiplier<FeeMultiplier>;
}

impl pallet_sudo::Config for Runtime {
    type RuntimeEvent = RuntimeEvent;
    type RuntimeCall = RuntimeCall;
}

/// Configure the pallet-template in pallets/template.
impl pallet_template::Config for Runtime {
    type RuntimeEvent = RuntimeEvent;
}
```

we create the runtime by the following pattern:

```
// Create the runtime by composing the FRAME pallets that were
previously configured.
construct_runtime!(
    pub struct Runtime
    where
        Block = Block,
        NodeBlock = opaque::Block,
        UncheckedExtrinsic = UncheckedExtrinsic,
    {
        System: frame_system,
        Timestamp: pallet_timestamp,
        Aura: pallet_aura,
        Grandpa: pallet_grandpa,
        Balances: pallet_balances,
        TransactionPayment: pallet_transaction_payment,
        Sudo: pallet_sudo,
        // Include the custom logic from the pallet-template in the runtime.
        TemplateModule: pallet_template,
        ContactTracing: contact_tracing,
    }
);
```

We can then compile the node in release mode whenever needed by running the following command:

```
cargo build --release
```

Also, we can start the node in development mode whenever needed by running the following command:

```
./target/release/node-template --dev
```

We can use the Substrate front-end template to interact with the node template by running the following command and open http://localhost:8000/ in a browser to view the front-end template:

```
yarn start
```

VITA AUCTORIS

NAME:	Farbod Behnaminia
PLACE OF BIRTH:	Isfahan, Iran
YEAR OF BIRTH:	1996
EDUCATION:	Isfahan University of Technology, B.Sc., Isfahan, Iran, 2019
	University of Windsor, M.Sc., Windsor, ON, 2023