CROSS-BLOCKCHAIN TECHNOLOGY FOR AN INTEROPERABLE AND SCALABLE DIGITAL CONTACT TRACING

Farbod Behnaminia and Saeed Samet

School of Computer Science, University of Windsor, Windsor, Canada

ABSTRACT

The COVID-19 pandemic emphasizes the significance of contact tracing for virus control but raises privacy concerns. Blockchain technology offers potential solutions, yet challenges exist for safeguarding sensitive information and enabling interoperability with other chains. This research explores using Polkadot's cross-blockchain feature for decentralized and privacy-oriented contact tracing. Our proposed solution stores personal data on a private blockchain, accessible to authorized entities only. Encryption ensures data security. Additionally, the Polkadot network's interoperability enables sharing data with health authorities or other blockchain networks. This study demonstrates the benefits and limitations of cross-blockchain contact tracing, urging further research and development. An effective and privacy-respecting contact tracing solution is attainable with the right approach.

KEYWORDS

Cross-blockchain Technology, Interoperability, Scalability, Digital Contact Tracing

1. INTRODUCTION

Utilizing blockchain technology, Digital Contact Tracing (DCT) records and monitors close contacts between individuals, safeguarding their personal information. The Polkadot network's cross-blockchain technology, particularly its interoperability feature, facilitates the establishment of a decentralized and distributed contact tracing system accessible to 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.

David C. Wyld et al. (Eds): SEAS, NLPI, SP, BDBS, CMCA, DMML, CSITEC -2023
pp. 79-94, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131708

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].

1.1. 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].

1.2. Cross-Chain Technology

Industry and academic institutions have paid a lot of attention to blockchains since the introduction of Bitcoin [3]. 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 [4].

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 [4].

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 [5].

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 [5].

1.3. 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 [6] 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 [6].

There are four distinct functions inside the Polkadot network [6]: 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 [6].

1.4. 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 [7].

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.

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 research 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.

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.

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 [8] 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.* [9] aims to introduce and review blockchain technology to the biomedical and health care areas, including its merits, drawbacks, and most recent applications.

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 [10]–[15]. 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.* [16] 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.

Some of the previous main works include Singapore TraceTogether, Google/Apple Contact Tracing, UK NHS Contact Tracing, China Health Code System [17]–[20]. 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. [7], 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.

S. M. Idrees et al. [21] 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.

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 [22].

3. Problem Statement & Methodology

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.

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 explore the potential applications of blockchain technology in patient tracking systems to address privacy-preserving concerns and mitigate the impact of the COVID-19 pandemic [23]. 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.

3.1. 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 [24]. 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 [25].

3.2. 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 [26].

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 [26].

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 [26].
Substrate nodes, at a high level, provide a layered environment composed of two primary components [26]:

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.

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.

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.

4.1. 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) [27].

4.2. 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 [26].

4.3. 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 **1** we can see the sequence diagram of mentioned scenarios and use cases.

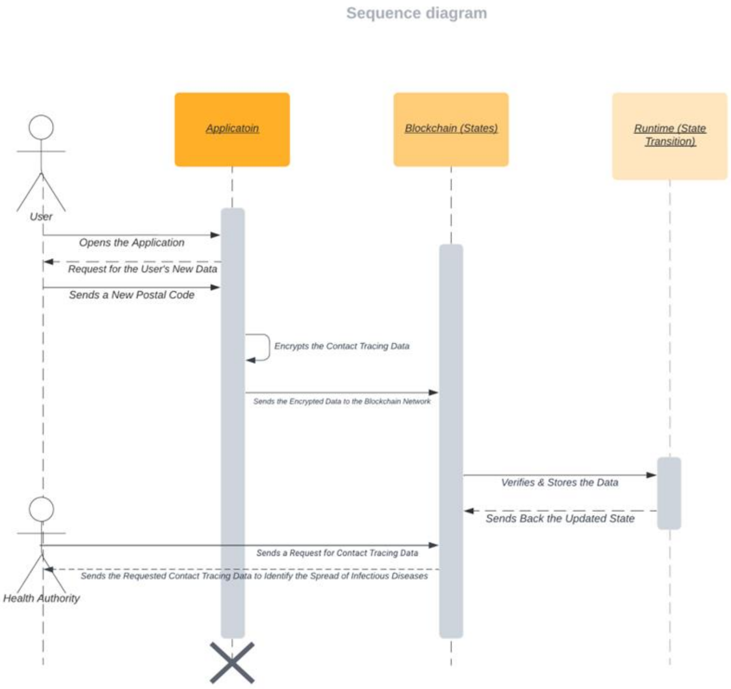
Sequence diagram
Applicatoin
Blockchain (States)
Runtime (State Transition)
User
Opens the Application
Request for the User's New Data
Sends a New Postal Code
Encrypts the Contact Tracing Data
Sends the Encrypted Data to the Blockchain Network
Verifies & Stores the Data
Sends Back the Updated State
Sends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

Figure 1. Sequence Diagram of Possible Scenarios

4.4. 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.

4.5. Security Analysis

Polkadot's security and privacy features are some of its most important characteristics and 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.

4.6. 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 in

is 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.

Table 1. Comparison between the proposed method and existing ones

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	✗	✗	✗	✗	✗	✓

5. Conclusions & Future Work

In this research, 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 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 [25].

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 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. 8.Human Resource Management: Contact tracing can be used to track the movement of employees and to monitor attendance and performance.

REFERENCES

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

[2] M. Swan, Blockchain: Blueprint for a New Economy. O’Reilly Media, Inc., 2015.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Decentralized Business Review, p. 9, 2008.

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

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

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

[7] 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 of Things Journal, vol. 8, no. 5, pp. 3915–3929, 2020.

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

[9] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” Journal of the American Medical Informatics Association, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

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

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

[12] R. Baldwin and E. Tomiura, “Thinking ahead about the trade impact of COVID-19,” Economics in the Time of COVID-19, vol. 59, pp. 59–71, 2020.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] J. Bay et al., “BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders,” Government Technology Agency-Singapore, Tech. Rep, vol. 18, p. 1, 2020.

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

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

[20] 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.

[21] 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 Medical Informatics, vol. 9, no. 2, p. e25245, Feb. 2021, doi: 10.2196/25245.

[22] 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.

[23] F. Behnaminia and S. Samet, “Blockchain Technology Applications in Patient Tracking Systems Regarding Privacy-Preserving Concerns and COVID-19 Pandemic,” International Journal of Information and Communication Engineering, vol. 17, no. 2, pp. 144–156, Feb. 2023.

[24] 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.

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

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

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