LICENTIATE THESIS

Blockchain and Distributed Hash Table Technology in Decentralized Systems

Morteza Alizadeh

Pervasive and Mobile Computing

LULEÅ
UNIVERSITY
OF TECHNOLOGY

Blockchain and Distributed Hash Table Technology in Decentralized Systems

Morteza Alizadeh

Department of Computer Science and Electrical Engineering
Luleå University of Technology
Skellefteå, Sweden

Supervisors:

Professor Karl Andersson, Professor Olov Schelén
Luleå University of Technology

To my family

Abstract

The Internet of Things (IoT) is one of the popular domains in real-time analytics, machine learning, ubiquitous computing, commodity sensors, and embedded systems where remote smart devices play notable roles in smart homes and industry. The information from emerging IoT environments like remotely-controlled objects, autonomous vehicles (AVs), and energy management can produce a huge amount of data. Moreover, understanding the security in a scalable decentralized IoT environment is a significant issue.

Decentralization has become popular again in the world since cryptocurrencies started to be a part of businesses. Therefore, researchers invested in upgrading resources to increase the reliability of these systems among people when most of the activities and human works are now managed by smart electronic devices remotely. Distributed ledgers, Distributed Hash Tables (DHTs), and blockchain technologies are proper decentralized technologies that improve system security, scalability, and trustworthiness. Blockchains contain a group of connected blocks that are digitally signed transactions stored in a decentralized fashion. The DHT technology is another decentralized solution that helps applications keep files and information immutable in a decentralized manner to mitigate the high cost of storage without memory limitations.

In this thesis, we argue for a decentralized systems paradigm and, in conjunction with IoT and the blockchain. Our contributions are as follows. First, we introduce the term networks and service architectures and how it is possible to use blockchain in the real world. We consider different architectures in IoT systems and show the blockchain encounter with the IoT and the resulting behavior. Second, we detect most of the frequent types of attacks in IoT related to using blockchain in the systems. We also describe how the blockchain works and illustrate a variety of security problems in systems. Furthermore, we discuss how the blockchain solves security problems by comparing different blockchains and explain how users handle their communication without third-party dependence. As our third contribution, we propose a novel architecture that consists of finding global identification in distributed applications and enable decentralized systems to be more secure with the help of blockchain technology. We also validate the proposed architecture and novel decentralized application development to evaluate high efficiency by combining blockchain, DHT, and biometric technologies.

Contents

Acknowledgments

I would like to thank my advisors. My sincere gratitude goes to Professor Karl Andersson for giving me the opportunity to become a PhD student and all the lessons I learned along my journey, both in professional and private life. I would like to thank my co-advisor, Professor Olov Schelén for the collaboration and support. Many thanks to my fellow PhD students and rest of the staff at the university.

This thesis would not have been possible without the support from our industrial partner and the Kolarctic CBC DIT4BEARS project. I had the pleasure to work with amazing colleagues.

Finally, and most importantly, I would like to thank my family. I love them and am proud to have such incredible people in my life.

Skellefteå, September 2021
Morteza Alizadeh

Part I: Thesis Introduction

Chapter 1

Introduction

1.1 Introduction

Internet of Things (IoT) is defined as a global infrastructure that involves many physical and virtual objects that are embedded with sensors, software, and other technologies to connect and exchange data over the Internet [49]. Many industries like automotive, railway, mining, utilities, healthcare, agriculture, manufacturing, and transportation are experiencing IoT benefits. Communication technology, such as 5G, will help to increase the use of the IoT [24]. There are over 1 billion cellular 5G-IoT connections in 2020, and Ericsson forecasts around 5 billion 5G connections by 2025 in the market [20]. Few examples of the wide range of emerging IoT applications are shown in Figure 1.1, including digitizing society (e.g. smart city, healthcare), automated industrial production, and digital currency.

Centralized systems are not suitable for some organizations. Bureaucratic leadership, remote control, delays in work, management of big scale systems, and bottlenecks can appear when the traffic spikes in the centralized systems. Also, disadvantages of centralized systems may include high dependence on the network connectivity, less possibility of data backup, and complex server maintenance. These leakage might convince user-based systems to move from centralized systems to decentralized systems. Still, keeping the system secure among different users is the most significant issue [23].

A distributed system is a system in which components are located in different places and interact to achieve a common goal. It should have no single point of failure and not depend on central servers. Facebook and the early version of email are famous examples of distributed systems. They communicate and coordinate their actions by sending and receiving messages directly to other parties [47]. A distributed system can manage many devices, applications, users, and IoT units. Resource sharing, concurrency, scalability, and transparency are the main advantages of this architecture [16].

Decentralized systems are by necessity distributed. They do not rely on any central party.

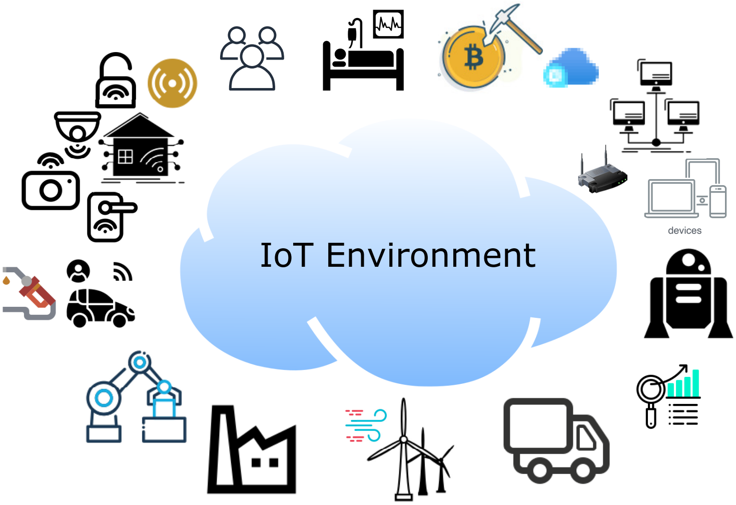


Figure 1.1: The emerging IoT use-cases.

IoT systems need to be designed decentralized when facing numerous devices and users [36]. Typically, such a system has multiple authoritative parties, each of which has special duties. This architecture solves problems such as scaling, the independence of central servers, and the extensive use of network traffic. In other words, decentralization is known as a software architecture in many references that includes two significant features, being no single point of failure and not being owned by any party. Although researchers are investigating new solutions to address scalability and security in decentralized systems, the double-spending issue considers the main security problem [4,5], which is significantly harder to solve in decentralized systems because of no trusted third party and multi-servers systems.

Several types of attacks exist to target millions of IoT devices [45]. IoT experts consider the possibility of security attacks in their architecture design. Therefore, they help to deploy secure IoT environments and applications in a decentralized manner. Although Google and Amazon as service providers presented a distributed and secured storage management [63], researchers are trying to find a distributed decentralized solution to avoid centralized data ownership.

The Peer-2-Peer (P2P) architecture offers decentralization without the need for mediators. P2P networking is a distributed application architecture that partitions tasks or workloads shared between peers [11]. Digital currency can be transferred from one user to another through a P2P network with the help of a distributed ledger called a blockchain.

Blockchains are decentralized systems that help to achieve immutable transactions and distributed consensus. The distributed ledger is information that is shared among several nodes in the network. Nodes replicate and keep the copy of the ledger. Distributed ledger technologies reduce the cost of trust [10]. It can help us decrease our necessity of governments, agents, clerks, and assent officers.

The immutability and consensus for each transaction do not rely on centralized authorities. Furthermore, they can be used as a security solution for IoT systems. IoT applications can complete transactions securely in non-editable and trusted environments with the help of the blockchains [17].

A Distributed Hash Table (DHT) is a technology to store data defined as data based on key-value pairs. This system works without any central coordination, so all nodes form the collective system decentralized. They are regularly fault-tolerant because they support replicated crossed multiple nodes data [53]. DHT can scale for large volumes of data over many nodes. Also, the data values can be of any form of data. DHT present a simple way to get information in an extensive collection of data. Also, nodes in a DHT can be easily added or removed without forcing a significant amount of re-balancing of the data in the cluster.

Interplanetary File System (IPFS) is a distributed and decentralized P2P system that is designed based on DHT technology [9]. IPFS can be used to store data and compile it in a decentralized fashion.

Identification issues and keeping data records secure are essential topics in applications that work based on IPFS and blockchain.

Thus, in this thesis, we define and model the combined machine learning face recognition solution based on a public blockchain and IPFS to answer security and identification problems. We model scenarios by explaining video conference applications as a use case. The public blockchain and IPFS are the solutions for decentralization. Besides, we consider the blockchain mechanism to manages transactions by its immutable historical data. IPFS supports decentralized web hosting and sharing data in a DHT without having to worry about memory limitations. Furthermore, the intelligent identification system can be beneficial for a decentralized system. Finally, this thesis illustrates architectures for video conferencing combining the blockchain and IPFS. We showed that the proposed solutions are feasible because of decentralized and immutable features.

1.2 Research Motivation

In this thesis, we considered three main research motivations, which are much obvious among other challenges. First, all traditional systems must change or be upgraded by new updated technology and knowledge. Second, centralized technologies should change their face to use new decentralized updated features. A decentralized system has many advantages and disadvantages. Although time and the security risk potentially rise by increasing the number of systems' members, this architecture helps to solve many problems, such as scalability, the independence of central servers, and avoid single point of failure that can be a risk factor for organizations [55]. Third, keeping the system secure and keep information immutable in a decentralized manner are advantages.

Decentralization. Decentralization means that the system should be designed decentralized, so that it has no central unit or any third party to control users' activity with the lowest amount of failure risk. Besides, this system must not be owned, controlled, and managed by a particular person or authority. Network. A P2P network without third party is an example of decentralized systems that parties can communicate directly to another party. Distributed ledger called blockchain transfers digital money from one user to another through a P2P network. The P2P architecture suggests decentralization, and most transactions are executed without the need for a third party. Today, P2P networks are at the core of distributed computing applications, cryptocurrencies, and blockchain. Bitcoin, Ethereum, and other cryptocurrencies are developed based on P2P and decentralized systems [27]. Developers who want to use these technologies must adapt their applications with decentralized technologies. So, industrial companies are trying to find a solution and upgrade their technologies to work and collaborate with this type of cryptocurrency and decentralized architecture.

Identification. A fundamental characteristic of an IoT environment is to have a powerful identification system. A P2P-IoT environment needs to know parties who communicate with the network and register all smart devices in a decentralized fashion [2]. All users should clarify their identity to the system. Identification in the centralized system is not a big and complex job. All identities who need to communicate with the network must be registered in the main server before. The problem is to answer how we can handle identification in the decentralized system without any single server or authority to manage the registration.

Immutable Storage. Secure data sharing and storage is another research area to consider when dealing with decentralized systems. In a decentralized system, all modules and sections must be decentralized. Unfortunately, cloud and servers are not fully decentralized [8]. Therefore we should find a way to upload and compile our scripts and applications using decentralized file sharing and storage. In public blockchain systems, where all transnational information can be stored on the network like a ledger, where all parties must keep a copy of this ledger, and nobody can delete or change it. Still, storing bulky data is a challenge in the blockchain, so IPFS technology as an immutable file storing system can be beneficial. This combination helps the system to have a decentralized architecture with a decentralized storage system.

1.3 Research Questions

This section presents the selected research questions based on the state of practice and state of the art review. The main thesis contribution is decentralized applications' development and evaluating their efficiency by combining Blockchain, DHT, and biometric technologies. In the following, we describe two research questions which this thesis attempts to answer:

RQ1: What are the security problems in decentralized Blockchain in general and in conjunction with IoT?

Security is the most significant parameter in all systems and involves protecting the system from viruses, outer attacks, and malicious behavior. In recent years the number of security attacks increased by presenting decentralization definitions and raising the number of IoTs. These attacks change their faces by presenting cryptocurrency and digital money. Although blockchain systems are secure systems naturally based on their definition, there are a rare number of new security problems that make them not as secure as before. Therefore, with **RQ1** we raise the need of extending the knowledge to include possible security attacks in decentralized blockchain in general and in conjunction with IoT.

RQ2: How can identification be provided in decentralized systems?

Applications are migrating from centralized to decentralized solutions for better performance without the need for third-party interactions. However, integrity, security, identification, and authentication problems are still universal in current decentralized systems. Current applications typically rely on decentralized systems to provide a stable and secure basis for executing tasks and processes. How new decentralized systems manage their users identification is a challenging issue. Therefore, with **RQ2** we raise the need for an architecture that models new identification schemes resulting from the combination of decentralized technologies.

1.4 Research Methodology

This section discusses about the research methodology that is used in this thesis work. The research methodology is a collection of the method to explain the problem analytically and systematically solving a research problem [33]. Surveys and other research techniques are the methodology's main components. Our research process follows the seven steps as shown in Figure 1.2, although slightly modified to serve our research context of implementing real-world solution.

To conduct a study, the following steps have been followed: 1) Define research questions; 2) Reviewing recent researches to find the gaps; 3) Formulate hypothesis to solve the problems; 4) System prototype development and implement technical solution; 5) Collect data and analyze the output; 6) Analyze the results, 7) Interpret and report the final result as a research article. Steps 4 to 6 are conducted iteratively to increase the efficiency of the output within an acceptable range. As an example the research process solving the second research question is outlined below.

Step 1 The research question is defined as detection of security issues in decentralized systems in relation to blockchain which is described in Section 1.3.

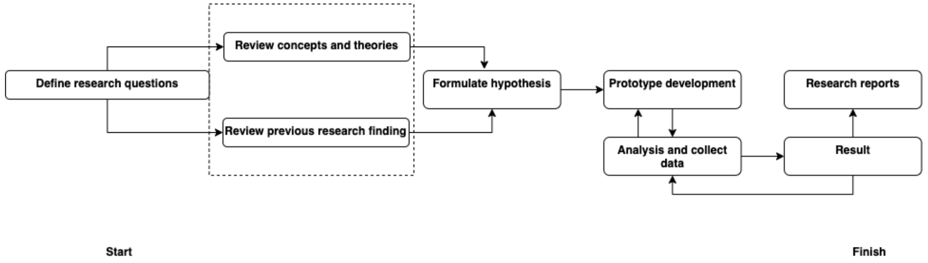

Define research questions
Review concepts and theories
Review previous research finding
Formulate hypothesis
Prototype development
Analysis and collect data
Result
Research reports
Start
Finish

Figure 1.2: The research process in this thesis

Step 2 Review and understand blockchain terminologies and learn from recent blockchain research to earn experiences and find out the important related works on blockchain and related applications.

Step 3 A hypothesis for using blockchain as a secure solution for events combined with IPFS to overcome the limitations was developed mentioned in Section 1.5 and Paper B and Paper C.

Step 4 A prototype was developed using a Javascript based mixed solidity which is presented in Papers B and C.

Step 5 To evaluate the performance, different parameters where measured, such as time and usage capacity being two main parameters to be evaluated performance that are mentioned in Papers B and C.

Step 6 The results were analyzed and the performance of solutions were compared with other solutions in different scenarios.

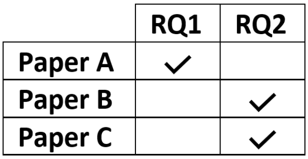
Step 7 After adequate results were generated and the hypothesis was validated, the results and findings were documented and submitted to a conference and a peer-reviewed journal, Papers B and C.

Better results with better performance were obtained by repeating step 4 to 5 many times.

The above research process presented technical solutions that are pre-selected parts of the proposed conceptual architecture and perform a preliminary analysis to validate the model in a decentralized manner.

1.5 Thesis Contribution

In this section we present the main contributions from this thesis. Figure 1.3 presents a high-level overview of the contributions in terms of the way our research results ad-



	RQ1	RQ2
Paper A	✓	
Paper B		✓
Paper C		✓

Figure 1.3: Mapping between the included papers and the research questions.

dress the stated research questions from Section 1.3. The main contributions include: (1) a review on different aspects of IoT systems in relation to decentralized systems like blockchain and finding the common solution for the security problem. (2) Developing an architecture that models an efficent blockchain and DHT based system that is scalable and resource efficient; and (3) Conducting a preliminary implementation of a decentralized identity system based on blockchain and IPFS technology for validating the proposed architecture.

In the following, we list the produced research results and then in detail discuss the individual contributions.

- **Paper A.** *A Survey of Secure Internet of Things in Relation to Blockchain.* **Morteza Alizadeh**, Karl Andersson, and Olov Schelen. Journal of Internet Service and Information Systems. Accepted on August 1, 2020.

  – Distributed ledgers and blockchain technologies provide immutable replicated histories of data to improve systems' security. Blockchain is a connected block of data containing digitally signed transactions, a cryptographic hash of the previous block, and a timestamp stored in a decentralized and distributed network. The Internet of Things is one of the application domains based on blockchain is discussed in this research. This article reviews the structure and architectures of distributed IoT systems and explains the motivations, challenges, and needs of blockchain to secure such systems. However, there are substantial threats and attacks to blockchain that must be understood and suitable approaches to mitigate them. We, therefore, survey the most common attacks on blockchain systems and assess how malicious these attacks are in the IoT context.

  – I was the main driver of the paper. I reviewed and analyzed the state of the art on IoT and Blockchain. I proposed comparision among security attacks. I wrote the complete paper. Karl Andersson and Olov Schelen, as my main supervisors, were taking part in the complete process of building the proposed definitions, contributing with constructive feedback and discussions that led to the current form of the definition. Also, they both helped with formulating the main message of the paper and commented the paper's text to improve its structure and presentation.

- **Paper B.** *Efficient Decentralized Data Storage Based on Public Blockchain and*

IPFS. **Morteza Alizadeh**, Karl Andersson, and Olov Schelen. IEEE CSDE. Published 2021.

- Blockchain technology has established a decentralized, tamper-proof, immutable, and ordered ledger of transactional events systems. Still, attempting to leverage these systems may be challenging when data storage requirements exceed most blockchain current capacities. Storing large amounts of decentralized data while maintaining system efficiency is the challenge that this research targets. This contribution introduces the IPFS technology to store information immutably and decentralized to mitigate the high storage cost. A storage system involving blockchain and other storage systems in concert should be based on immutable data and prevent data removal from malicious users in the DHT. System efficiency improves by decreasing the overall processing time in the blockchain with the help of DHT technology. Introducing an agreement service is another research proposal that communicates with the blockchain via a RESTful API. This contribution shows the proposed method's applicability and concludes that the combination of IPFS and blockchain provides efficient cryptographic storage, immutable history, and overall better efficiency in a decentralized manner.
- I was the main driver of the paper. We wrote the complete paper that designed the proposed architecture and outlined it to the new smart trading case study in a decentralized fashion. Karl Andersson and Olov Schelen were involved in developing the proposed architecture, supervising the work, and providing constructive feedback and discussions that led to the current version of the architecture.

- **Paper C.** *Blockchain-based Smart Identification for Video Conferencing.* **Morteza Alizadeh**, Karl Andersson and Olov Schelen. Blockchain: Research and Applications magazine, submited in 2021.

  - Video conferencing applications are a common way to provide a significant and consistent basis for virtual conferences. However, integrity, security, identification, and authentication problems are still universal. The recent video conference technologies typically rely on web services to provide a stable and secure basis for executing tasks and processes. These video conferencing applications are migrating from centralized to decentralized solutions for better performance without third-party cooperation. This research demonstrates a decentralized smart identification scheme for video conferencing applications based on biometric technology, machine learning, and a decentralized hash table combined with blockchain technology. After identifying users by implementing machine learning functions, we store users' information on a DHT and event logs on the blockchain network. Finally, we introduce three architectures to leverage blockchain technology's immutability and traceability features to secure storage and search for event data. The experimental results

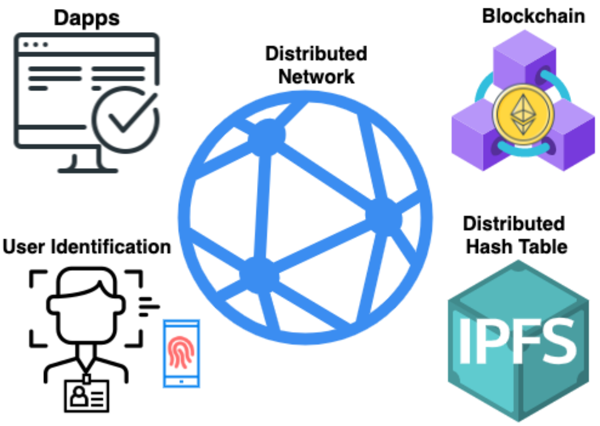


Figure 1.4: Decentralization Main Components.

represent an architecture based on blockchain and DHT in more secure and scalable solutions but this model takes longer time to execute than two other architectures using a centralized database.

Figure 1.4 shows a very high-level decentralized system. The network includes multiple subsystems such as applications, identification, blockchain, and IPFS. First, users must clarify themselves through the network. Then, users need to sign in to the system by identifying themself. Users' information can be stored on IPFS, and event logs are stored on the blockchain network after identifying users using machine learning identification. Blockchain technology helps to keep immutability and traceability features to secure storage and search for event data. Also, IPFS helps to store bulky data, upload and compile scripts as a decentralized web hosting node.

– I was the main driver and contributor to the paper. I initially designed the study with the primary plan to develop a decentralized video conferencing demonstration for the experiments. I also developed the machine learning model while we jointly performed the smart identification based on biometrics information. As my main supervisors, Karl Andersson and Olov Schelen, were taking part in the complete process of building the proposed definitions, contributing with effective comments that drove to the current version of the report. Also, they both helped formulate the paper's main message and commented on the paper's text to improve its structure.

1.6 Chapter Summary

This chapter introduced the main topic of the thesis, followed by a detailed discussion of the research motivation. Accordingly, we discussed the main research challenges that we identify from the state-of-the-art in blockchain and decentralized systems. Further, we defined and described two research questions that we attempt to address with this thesis, focused on defining the architecture of IoT systems and security solutions without memory limitations in decentralized systems. Then, we described the research methodology we utilized for this thesis, which consists of seven steps. Finally, we listed the main thesis contributions that emerged from our research, with related papers discussing how each thesis contribution addresses the proposed research questions.

Chapter 2

Background and Related Work

In this chapter, we discuss the background of the technological concepts used in this thesis and terminologies related to it and discuss in greater detail the relevant related works.

2.1 Background

Section 2.1.1 presents the architecture of the IoT development. Special attention is given to IoT security, giving an overview of network designs that we utilize in our first contribution. We describe blockchain and its main components in Section 2.1.2. Then, in Section 2.1.5 we cover the fundamentals of identification problems in the decentralized systems, with the most prominent definitions and scenarios. We also discuss state-of-the-art smart identification in Blockchain based systems by analyzing the related works in Section 2.2.

2.1.1 Internet of Things (IoT)

The term IoT was coined by Kevin Ashton, executive director of the Auto-ID Center [7], representing the network of electronics devices known as things [1]. Things are equipped with sensors and software that connects and exchanges data with other devices through the network over the Internet. Smart cities, mobile networks, control systems, and automation (including home and vehicle automation) are common IoTs examples. The IoT formulates possibilities for more direct integration of the physical world into remote-based systems with mobile technology, resulting in efficiency improvements, economic benefits, and reduced human exertions. Although there is severe substantial attention about dangers in the growth of IoT devices, especially in privacy and security, IoT helps to increase Internet usage for a better and accessible smart future.

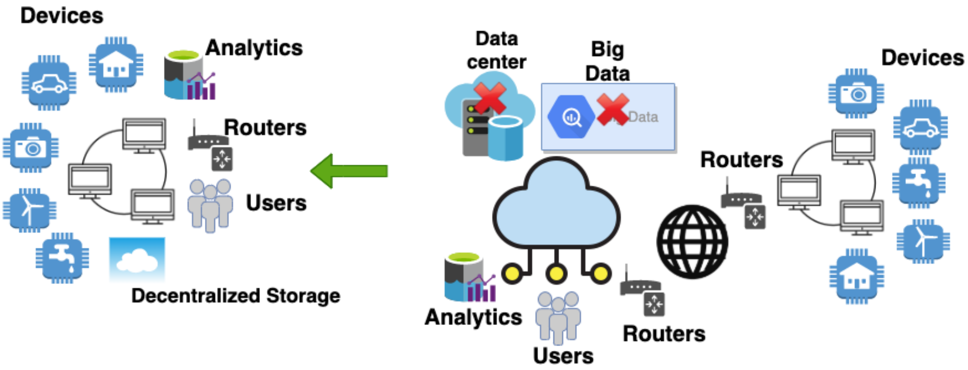


Figure 2.1: Decentralization of a distributed system

Decentralization Versus Distribution

Distributed systems consist of applications, users, workstations, and IoT devices achieving resource sharing, concurrency, scalability, and transparency. Accordingly, IoT systems perform communication in a decentralized or distributed fashion to increase their performance when encountering numerous sensors, users, and computational elements [50]. Most of recent distributed systems can switch to be decentralized systems just by upgrading the traditional databases and remove the centralized point like datacenters that is illustrated in the left side of Figure 2.1. Typically, a distributed system is fully connected, where parties are located in different places. Moreover, all system parties can communicate and coordinate their actions by sending and receiving messages directly to/from other parties. Authoritative parties serve a subset of the workload. Therefore, the security risk potentially grows by increasing the number of parties in these large systems. Clouds are example of a service that helps IoT-based systems. The right side of Figure 2.1 illustrates a high-level view of distributed systems that cloud is one of the main components. Clouds are used to help datacenters to be available to many users over the Internet. The cloud architecture solves scalability, the independence of central servers, and the extensive use of network traffic.

Challenges

The IoT involves several principal challenges that are explained in the following content.

- **Accessibility.** Today, electronic devices are equipped with modern and robust hardware. Accessibility is used for specific hardware or software that was designed to make it easy to use. In addition, applications should be designed to make technology less challenging for those with disabilities.

- **Scalability.** Scalability is the system's ability to manage more tasks after adding more resources, which means that the system can control the number of parties who want to store data that need resources such as hard drives, processors, and server-side memory [13].

- **Availability.** Availability is a goal that indicates delivery of services consistently in quality or performance, meaning that the quality of being present or ready for immediate use and working without interruptions [12]. In a system with high availability, the failure of a single section or part of the equipment should not significantly negatively impact network performance.

- **Data Security.** Data security implies preserving digital information from unauthorized access and malicious activity during its entire lifecycle [30]. Therefore, the information needs to be secured by multi-level protection. Encryption and data masking are the common solutions. Thus, data security emphasizes information security from hardware, software, storage devices, access control, and the security of software applications.

- **Trust.** The term trust is about protection from untrusted components modification. Users do not prefer to join a system with uncertainty when the application cannot convince users to be qualified. Therefore, applications need to be designed well to feel that communication and document sharing are safe by accepting applicable policies.

- **Flexibility.** Flexibility means that one application can add to and cooperate with other applications. Additionally, updating these applications should not be complex. Therefore, flexible modular applications can be easily accepted and connected to other modules.

- **Manageability.** Financial costs or manageability include nonrecurring material costs and recurring network operational costs. Furthermore, a decentralized system should carry the maximum traffic for a given financial cost and less time consumed.

- **Performance.** Decentralized systems must be compatible with various applications and provide reasonable response times from P2P devices. Moreover, they must work all the time without interruption. Also, they need to continue to handle tasks during equipment failure and system overloads. Additionally, the systems should be simple to modify and update, such that obtaining and solving problems should not be too time-consuming. Therefore, many different parameters are related to measuring decentralized systems' performance.

  A high-performance decentralized system must have all mentioned parameters at a reasonable level. This performance is the primary purpose of system design. Other requirements are about discovering the features and functions that need to be identified earlier, such as performing a network-readiness assessment and creating a project plan.

2.1.2 Blockchain

The distributed ledger is information that is shared across several parties of the distributed network. All parties receive replicated and preserved duplicate copies of the ledger. The ledger is stored on each node separately after all parties accept the current version of the information. Thus, distributed ledger technologies overcome the trust issue. The distributed ledgers can help us reduce our need for governments, agents, assistants, and assent officers.

Blockchain is an environment that shares an immutable digital ledger of transactions as digital information in a distributed network. This property makes it difficult or impossible to change, hack, or cheat the system. Also, this distributed ledger provides immutability, trust, and data security [34]. This environment is required for cryptocurrencies, record keeping, digital notary, and smart contracts.

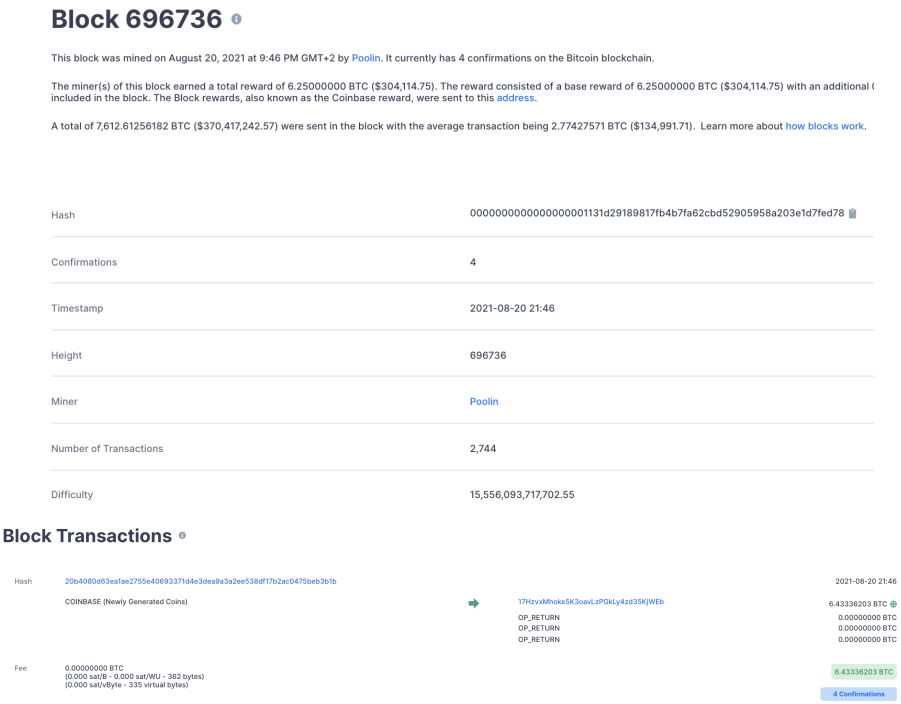
Blockchain is a structure that looks like a chain. It contains a set of blocks where each block is a data package. The data in each block contains a timestamp and a hash code, whereas each block knows the previous hash code. This theory helps to understand how a chain of blocks is formed, similar to parents and children. The chain length grows while adding new blocks. Thus, chained blocks represent a complete ledger of the transaction history. It is reasonable to return to the genesis block by following the parents' hashed addresses. This chaining theory ensures the trust of the whole blockchain. These hashed values are specific for each data record.

A block is made up of a number of transactions. A block with its transactions form an authoritative and global ordering on all transactions. A miner is a network's party that chooses a list of transactions and works on them to ”solve” the block. After that, it broadcasts the block to the network, and all the transactions in the block become confirmed. The adding new block process finishes when most of the miners in the network accept it by a consensus mechanism. When a new block is added to the ledger, the information inside the confirmed block turns to an immutable record.

A hash value is the output of a hash function that can be used to map data of arbitrary size to fixed-size values. A hash function is a one-way function, and the same data will always produce the same hashed value. A hash is used to encrypt demands needed to solve a blockchain computation. It is almost impossible to decode the hash if someone was trying to crack the blockchain.

Anatomy of a Block

Bitcoin is an example of blockchain, cryptocurrency, and P2P electronic cash systems. Bitcoin block memory is limited to one megabyte of data [32]. A block contains a block hash address, timestamp, address of the previous block, the hash of the root of Merkle tree of all the transactions in the current block, difficulty target of the current block (meaning how difficult the target hash will be to find), miner name, and Nonce. Moreover, a transaction contains a version number, transaction inputs/outputs, and the amount of bitcoin as shown in Figure 2.2.



Block 696736

This block was mined on August 20, 2021 at 9:46 PM GMT+2 by Poolin. It currently has 4 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($304,114.75). The reward consisted of a base reward of 6.25000000 BTC ($304,114.75) with an additional (included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 7,612.61256182 BTC ($370,417,242.57) were sent in the block with the average transaction being 2.77427571 BTC ($134,991.71). Learn more about how blocks work.

Hash	000000000000000000001131d29189817fb4b7fa62cbd52905958a203e1d7fed78
Confirmations	4
Timestamp	2021-08-20 21:46
Height	696736
Miner	Poolin
Number of Transactions	2,744
Difficulty	15,556,093,717,702.55

Block Transactions

Hash 20b4080d63ea1ae2755e40693371d4e3dea9a3a2ee538df17b2ac0475beb3b1b 2021-08-20 21:46

COINBASE (Newly Generated Coins) ➡ 17HzvxMhoke5K3oavLzPGkLy4zd35KjWEb 6.43336203 BTC

OP_RETURN 0.00000000 BTC
OP_RETURN 0.00000000 BTC
OP_RETURN 0.00000000 BTC

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 362 bytes)
(0.000 sat/vByte - 335 virtual bytes)

6.43336203 BTC

4 Confirmations

Figure 2.2: Block and Transactions in Bitcoin

Consensus in Blockchain

Consensus is a process to authenticate and validate a value or transaction on a distributed ledger without the need to trust or rely on a central authority. Therefore, consensus mechanisms are the fundamental property of any blockchain or distributed ledger. Most blockchain platforms utilize one of the below mentioned common consensus algorithms: Proof of Work (PoW); Proof of Stake (PoS); and Delegated Proof of Stake (DPoS) are three common mechanisms that try to form a secure environment for transactions or replicas by the use of consensus protocols to ensure all that replicas of the shared agreement are secured.

In the PoW mechanism, miners solve complex cryptographic mathematical puzzles, take rewards with a certain amount of Bitcoins, and create a new block. In the PoS mechanism, there is no block reward. The creator of a new block is chosen depending on its wealth defined as stake, and the miners take the transaction fees. DPoS is an updated version of PoS. In DPoS, token holders do not work on the block validation. Instead, they select delegates to do the validation. The token holders can vote delegates out and replace them with other selected delegates when they miss their blocks or publish invalid transactions. This process is partially centralized and faster than any other consensus algorithm [62].

Blockchain Categories

Permissioned blockchain is one type that a limited number of known trusted participants carry a copy of the blockchain's ledger. Researchers categorized this type of system into private and consortium categories. Private and consortium blockchains allow only a few known members to keep a copy of the entire blockchain or ledger. Moreover, miners are delegated by members, so the security is at an acceptable level. Due to the characteristics of the permissioned blockchain, related applications tend to be more secure and faster. Additionally, they are centralized.

The second one is permissionless or public blockchains. They allow anyone to keep a copy of the blockchain and be included in the validation process to publish new blocks. They usually work on digital currencies like Bitcoin. Therefore, all members have the right to collaborate with the system or manipulate the mining protocols to help verify transactions.

2.1.3 Comparison of Public, Consortium, and Private Blockchains

Table 2.1 shows the properties of three types of blockchain. A consortium can be set up to be a more public or private blockchain. When the system needs to have a high distribution level, it is better to use a public blockchain. In the private blockchain, parties on the network do not need to pay for services. In addition, a consortium blockchain is flexible. The system can be more private or more public and can have multiple centralized parties.

Criteria	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus Determination	All	Multiple Organizations	One Organization
Read permission	Public	Can be Public or Restricted	Less Public or Highly Restricted
Immutability	Nearly Impossible to Tamper	Can be Tampered	Can be Tampered
Identity	Pseudo-Anonymous	Approved Participants	Approved Participants
Distribution	High	Medium	Low
Consensus	Permissionless	Permissioned	Permissioned

Table 2.1: Comparison of public blockchains, consortium blockchains, and private blockchains

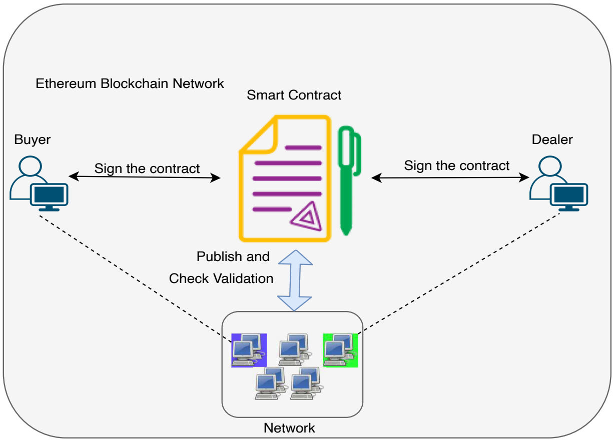


Figure 2.3: Digital Trade by Public Blockchain

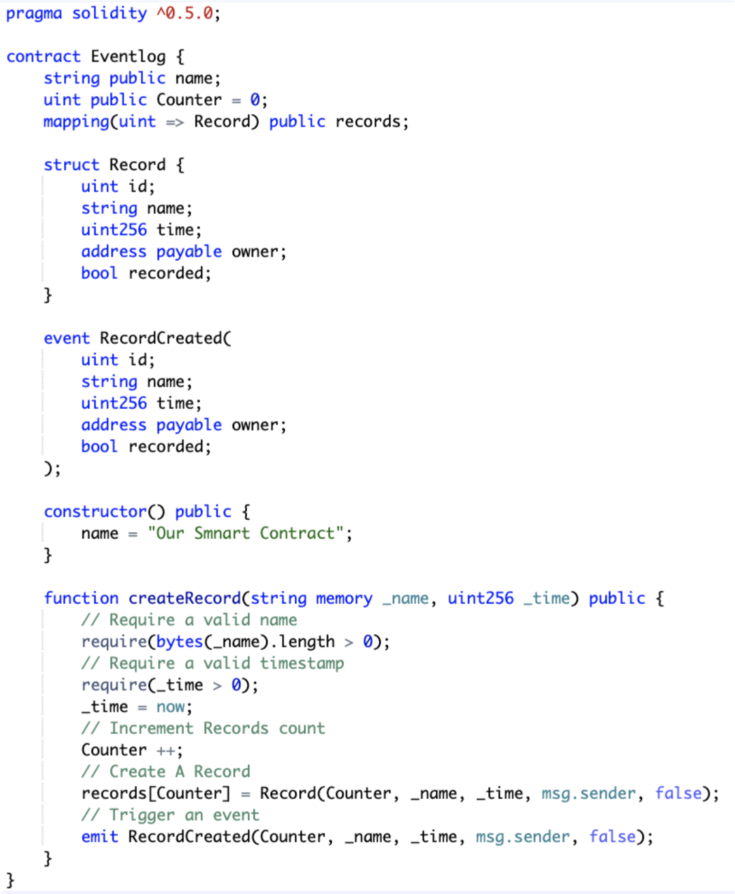
Smart Contracts

Smart contracts are electronic contracts that provide the connection of trustworthy transactions without third parties intervention. These transactions' descriptions share on the blockchain network, which is trackable and immutable. Smart contracts are used to transfer cryptocurrency, investments, trading, or other use cases in e-commerce. For example, the parties can transfer money by an application, and this money can be transferred among other parties or forwarded to another person. These systems store their contracts as a ledger on the network. Figure 2.3 shows two sides of a negotiation on a smart contract to sign and publish it on the smart ledger. Then, a transaction stores all information, including user signatures, addresses, timestamps, and smart contract terms.

Figure 2.4 demonstrates a smart contract to store information. It includes a Solidity class that is a data structure and functions to record data on a smart ledger. Solidity is a programming language for smart contracts, and Ethereum blockchain can compile and deploy them.

Cryptocurrency Wallets

Cryptocurrency wallets are applications connected to blockchain networks on the parties electronic side that store parties' secret keys. They are used to sign and confirm digital transactions for blockchain-distributed ledgers by the parties in both sides of the transaction. They can be more than a keeper of cryptocurrencies. They can describe parties' professional and financial status or they can even be the identity. Metamask is a famous wallet for Ethereum blockchain [46].



```
pragma solidity ^0.5.0;

contract Eventlog {
    string public name;
    uint public Counter = 0;
    mapping(uint => Record) public records;

    struct Record {
        uint id;
        string name;
        uint256 time;
        address payable owner;
        bool recorded;
    }

    event RecordCreated(
        uint id;
        string name;
        uint256 time;
        address payable owner;
        bool recorded;
    );

    constructor() public {
        name = "Our Smnart Contract";
    }

    function createRecord(string memory _name, uint256 _time) public {
        // Require a valid name
        require(bytes(_name).length > 0);
        // Require a valid timestamp
        require(_time > 0);
        _time = now;
        // Increment Records count
        Counter ++;
        // Create A Record
        records[Counter] = Record(Counter, _name, _time, msg.sender, false);
        // Trigger an event
        emit RecordCreated(Counter, _name, _time, msg.sender, false);
    }
}
```

Figure 2.4: Smart Contract

Decentralized Applications

Decentralized Applications (DApps) are computer applications that work on a decentralized system. DApps can be a blockchain based application and a distributed ledger technologies such as the Ethereum blockchain, explicitly referred to as smart contracts. There are many DApps that have been developed during recent years based on the Ethereum platform [38].

An interesting example is decentralized video conferencing applications to sustain business purposes during the Covid-19 pandemic [43]. Furthermore, companies now realize the many interests of updating these applications to a decentralized form without any third parties intervention. For example, video conferencing involves a technology to communicate via electronic devices and allows users to continue face-to-face meetings in different locations without gathering in a single area. So, a DApp can help identify users who want to join a meeting without the help of a third party. This technology is especially appropriate for academic and business users in different places to save time, expenses, and hassles associated with travel.

2.1.4 Distributed Hash Table

A hash table is an associative array abstract data type that is known as a data structure. It has a structure that can map keys to values. A hash code is an output of a function that computes an index into an array of buckets from which the desired value can be obtained. Hash tables are convenient for storage and speed of access. The average execution time of any process is independent of the data size. Hash tables work based on the key-value storage method. Hashing and collisions are two main processes in the building of hash tables [57].

Hashing is a process that uses a hash function to get the key for the hash table and transform it into an index that will point to different arrays of buckets, which is where the information will be stored. The hashing function determines where to store and where to find it inside the hash table. Therefore, a good hash table must have a good hash function. Collisions are a big part of hash tables. A collision happens when the hash function shows a hash key for an occupied place. Therefore, avoiding collision is related to a good hash function. This function should be easy to compute and must share the keys uniformly.

DHT means that the entire table is distributed across different locations [9]. IPFS is a decentralized system with no single point of failure that works based on distributed hash table technology [53].

Kademlia is a distributed hash table that is established following peer-to-peer computer networks in 2002 [37]. IPFS uses Kademlia technology to recognize which nodes have which data. It presents a lookup service based on key-value pairs, which are stored in a DHT. Thus, all network members can retrieve the value associated with a given key with the minimum time to re-distributing keys.

IPFS is known as a decentralized storage protocol that is designed to address excessive file redundancy. The output of IPFS is a unique hash for each stored file. Users can retrieve the file by compiling the corresponding hash address with the help of the IPFS gateways. Thus, IPFS helps store files decentralized and immutable.

The main property of IPFS is that it stores data without considering the size of the data [3]. The data divides into many small parts, where each part is identified with its hash address called CID. These parts are distributed among other nodes that are as close as to the publisher node. All the parts can be combined again to recreate the main object after visiting the small parts when any user calls a query request. IPFS has command line and graphic interfaces that make performing uncomplicated for amateur users in all operating systems.

2.1.5 Smart Identification

Identification in Computer Science means the process of naming entities. Identities help systems verify that a person is whom they say. National identity numbers are examples of an identification type in a country. Smart identification is an application that is equipped with a mechanism to identify the objects for Web-based applications. The current applications use the help of famous third-party identifiers, like Facebook to identify objects when users try to register or sign in to the system.

2.1.6 Machine Learning

Artificial Intelligence (AI) is the knowledge that is represented by machines. It is a similar version of simulation of human intelligence in machines. AI methods necessitate machines to learn from experiences, show the correct reaction to the events, think like a human's brain, and mimic their actions [48].

Machine learning (ML) is a technique to achieve artificial intelligence purposes. It is an area of Computer Science that can learn from data, recognize patterns and make decisions based on their gained knowledge without direct human intervention. ML is designed based on the idea that systems can get knowledge from their experiences or history. Therefore, it can automatically learn from gained data, such as supervised and unsupervised techniques. For example, machine learning has been used in conjunction with sensor networks like IoT, driver assistance for smart cars, smartphones face and voice recognition, and intelligent assistance in smart devices like Siri in Mac OS and Cortana in Windows OS [31].

Face recognition is one of the ML technology use cases based on finding a match of a human face from a stored image or video. Authentication technology is a famous example that works by extracting and measuring face features from a given image.

Some technologies are designed to produce an application that covers face detection and face recognition procedures. Web Real-Time Communication (WebRTC) and Jitsi are two popular video conference applications. They are free and open-source technologies that provide web browsers and mobile applications with real-time communication properties [29]. It has an extremely fast no-server P2P communication. Currently, almost all browsers support these technologies [29].

2.2 Related Works

This section presents the related research in the field of Blockchain, IPFS, and decentralized identification.

2.2.1 Related Work on IoT

Previously, various studies have been carried out to develop scalable IoT architectures and deal with security issues.

Arellanes et al. [6] proposed new IoT service composition mechanisms for solving the scalability issue in IoT systems. They described that the number of connected things is quickly growing into complex workflows. Therefore, scalability in terms of the size of IoT systems becomes a significant concern. So, they reviewed and evaluated a framework of IoT service composition mechanisms to determine how well they fulfill the scalability requirements of IoT systems. Palattella et al. [44] analyzed 5G technologies for the IoT by studying the technological and standardization aspects.

Hassija et al. [26] reviewed the security challenges and sources of threat in the IoT to achieving a high degree of trust in the IoT applications. They consider different IoT use cases and emphasized security importance in these systems. Furthermore, they mentioned different types of security threats in the different layers of the IoT environment. They described how the blockchain theory could help solving the security issue and how to use fog computing concerning IoT to overcome those security threats. They explained that edge computing provides various features to increase the security and performance of IoT applications, and ML techniques represent an essential part in increasing the deduction accuracy and securing IoT devices vulnerable to denial-of-service (DoS) attacks. In this research, blockchain, fog computing, edge computing, and machine learning are discussed to increase the level of security in IoT.

Mosenia et al. [40] attempt to provide a comprehensive list of vulnerabilities and countermeasures against security threats on the edge-side layer of IoT. They first described three IoT models and defined security in the context of IoT. Then, they showed the possible attackers' potential motivations, discussed different types of attacks, and described possible countermeasures against them.

Liang et al. [35] described a DoS attack on an IoT system. They launched this attack by three different methods and compared these three DoS attack methods. Sinha et al. [52] proposed a solution to address the problem where non-statically preconfigured IoT devices try to gain access by asking permission/authorization. They also tested solutions to provide escalated permission to act in a controlled order. Eskandari et al. [21] presented an intelligent intrusion detection system (IDS) to protect the IoT devices. It is helpful to detect cyber threats as close as possible to the corresponding data sources. Also, it can detect various types of malicious traffic, including port scanning, HTTP and SSH Brute Force, and SYN Flood attacks with very low false-positive rates and satisfactory accuracies. Hao et al. [25] proposed the FastPay method that protects payments in blockchain-backed edge-IoT systems from double-spending attacks in the context of fast payments.

2.2.2 Related Work on Blockchain

The blockchain system is a decentralized system that stores transactional records in the immutable environment.

Christidis et al. [14] reviewed the blockchain mechanism. They believed that the combination of blockchains in the IoT domain would cause significant transformations across several industries. They described smart contracts as the main conjunction. Furthermore, Negara et al. [42] published a literature review on smart contract applications in various domains. Permissioned and permissionless are two broad categories of the blockchain. Therefore, it is necessary to know which one is a better solution for the specific system targeted. Helliar et al. [28] explored the barriers and drivers of diffusion associated with permissionless and permissioned blockchains, and they discovered limitations of permissionless and permissioned blockchains. Furthermore, they found that these two types of blockchains are not the same, and they affected diffusion in different ways.

Zeng et al. [61] offered a consortium blockchain to improve the regulation of the P2P lending market. This partially decentralized consortium blockchain can well improve transparency and security. They showed that this blockchain is suitable for financial regulation with limited pre-set nodes. Also, they considered safety, reliability, scalability, efficiency, and transparency to compare public and consortium blockchain. Yang et al. [59] explored the feasibility of applying both public blockchain and private blockchain technologies in different industry cases.

Wang et al. [58] described that consensus algorithms are the central part of blockchain systems. They tried to show different works that demonstrate consensus algorithms in distributed systems.

There are many surveys and review papers that show the blockchain cryptocurrency challenges [41]. Farell [22] analyzed the cryptocurrency in the industry with a particular analysis of Bitcoin in his thesis.

2.2.3 Related Work on Decentralized Systems

Ye et al. [60] addressed IPFS combined with blockchain to propose a system that stores vehicle data safely and efficiently. Moreover, they described the importance of vehicle data as a part of IoT that has become very important to store them safely. Still, security and capacity issues exist to store data safely and efficiently in decentralized systems.

Ul Haque et al. [56] used IPFS as their data-sharing infrastructure. They used public blockchain technology for transferring data in a P2P network to transport pre-trained deep learning models to others.

Shah et al. [51] presented a combination of blockchain and cloud technology to mitigate data security, privacy, availability, and resource utilization.

Tenorio et al. [54] proposed a framework for the design of decentralized systems to achieve data access, data provenance, and data discovery by suggesting a set of guidelines to combine blockchain technology and IPFS. They explained that other technologies, such as IPFS, are sufficient to use as a part of a decentralized system.

2.2.4 Related Work on Identification

Mohanty et al. [39] have focused on participant identification and authentication. Dargan et al. [15], and Elgharib et al. [19] found that there is a need for better applications and that new applications have acceptable features using ML for identification and authentication, like face recognition, fingerprinting, and IRIS.

Self-sovereign identity (SSI) is an approach to digital identity that gives individuals control of their digital identities. This solution is known as a good way without privacy leakage. Dunphy et al. [18] explained an emerging landscape of distributed ledger technology (DLT) based identity management (IdM) and evaluated three representative proposals: uPort; ShoCard; and Sovrin.

2.3 Chapter Summary

This section reviews the background and related work on the two main topics covered in this thesis: the Internet of Things (IoT) and decentralized systems. Then, this chapter starts to introduce IoT and decentralized systems like Blockchain and DHT.

The background section starts with a description of the IoT and its challenges, including communication, scalability, management, and security issues. Then, it described decentralization and showed the main components in the blockchain. Following, this chapter explained another decentralized system that works based on hash table technology, IPFS. It illustrates the most challenging problems in a system that combined blockchain and IPFS. Various related research studies on IoT, permissionless Blockchain, IPFS, and identification were presented at the end of this chapter.

Chapter 3

Contributions, Conclusion and Future Work

In this chapter we cover the contributions and conclude the thesis in light of the presented research questions and thesis contributions. In addition, we provide research directions for future work.

3.1 Thesis Contributions

This thesis makes three contributions. The first answers the first research question, while the second and third contributions provide answers to the second research question. The first contribution discusses recent research in IoT systems and their common challenges when IoT is combined with the blockchain. The second contribution is about models to combine blockchain and distributed hash tables to achieve better efficiency. The third contribution is about solving the decentralized identification problem, using ML algorithm techniques for a video conference application. The overall focus of this thesis is to propose decentralized, scalable models to overcome the scalability and security issues in decentralized systems like blockchain and distributed hash tables, which we address with details in the following contributions:

Contribution 1 - A Survey of Secure Internet of Things in Relation to Blockchain.

In the first contribution, we presented a survey of networks and service architectures and explained how blockchain could be used to answer the first research question. Then, the properties of the permissioned and permissionless blockchain were discussed. Designing and producing a secure blockchain-based IoT system that satisfies the users is essential. Then, we explained how the blockchains work, and covered their main components. Later, we showed the significance of privacy and security issues in decentralized systems. Furthermore, we reviewed three types of blockchains showing how they deal with security problems. Finally, we described consensus algorithms used explicitly for each blockchain and explained how users communicate through the decentralized system without third parties intervention.

Contribution 2 - Efficient Decentralized Data Storage Based on Public Blockchain and IPFS.

The second contribution answers the second research question. Recent decentralized applications need to have reliable data storage and an essential requirement for applications that help convince the digital world's users to accept them. Performance issues and data storage capacity limitations are therefore two popular issues that attract the researchers' attention. In the second contribution, we presented a combined solution based on a public blockchain and a DHT. Moreover, we explained how the blockchain manages several transactions by its immutability. Finally, this contribution demonstrated two scenarios of data storage based on mutual agreements in IPFS and blockchain systems. We also showed the second model encounter the decentralization and scalability issues.

Contribution 3 - Blockchain-Based Smart Identification for Video Conferencing.

The third contribution answers a question that arises as a follow up to the second research question, which is developing a model to increase the efficiency for decentralized applications.

The security and identification issues are requirements for decentralized applications that help satisfy the digital world's expected requirements. This contribution presented a combined machine learning face recognition solution based on a public blockchain and IPFS. We described video conference applications and how the blockchain manages transactions. Moreover, we discussed decentralized web hosting and sharing data in a DHT or IPFS. The question is how we can identify users. The IPFS decentralized web hosting environment is an excellent solution to keep most systems decentralized without thinking about blockchain's memory limitations. Finally, we model two video conferencing scenarios combining blockchain and IPFS with decentralized property and immutable features. Although the blockchain is an excellent solution to keep transaction data immutable in this contribution, it cannot answer the research question alone. This contribution is needed to cover multi-user identification and user privacy issues.

3.2 Thesis Conclusion and Future Work

This thesis has reviewed several research challenges concerning extending the definition of scalability and security in a decentralized manner. First, we explained the methodology for our study, and we started our research by reviewing and presenting two research questions. Then, we showed scalability and secure data storage as two major research motivations. Next, this thesis showed recent research in IoT systems and their common challenges when decentralized applications are combined with the blockchain and DHT. Moreover, we proved this combination that had better efficiency by presenting a video conference applications concept. It uses ML algorithm techniques to solve user identification problems in a decentralized fashion. Finally, we showed our models overcome the scalability and security issues in decentralized manner.

There are several directions for future research in order to complete and advance the work presented in this thesis. The most immediate future work is related to the second and third contribution. The following can be considered as the future of this research.

We intend to further evaluate the proposed model in the second contribution, which is needed to increase the security and scalability of decentralized systems. In addition, this investigation is required to better understand the reliability of the proposed model-based IPFS and Blockchain. Finally, the developed blockchain-IPFS model needs to be further tested by using more different scenarios to better evaluate their efficiency.

Many IoT systems are currently being migrated to decentralized systems that must manage a huge amount of transactions. Therefore, security and transaction order must be taken care of in such systems. The blockchain can solve the issue in many cases, but there are some limitations and leakage in these systems. Moreover, finding the best smart contract and storage limitation are considered two of the challenges in the blockchains. Although distributed hash tables can help mitigate the storage limitation, large-scale IoT systems need to be researched further to increase the efficiency of these systems.

References

[1] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[2] Alanoud Alhussain, Heba Kurdi, and Lina Altoaimy. Managing trust and detecting malicious groups in Peer-to-Peer IoT networks. *Sensors*, 21(13):4484, 2021.

[3] Morteza Alizadeh, Karl Andersson, and Olov Schelén. Efficient decentralized data storage based on public blockchain and IPFS. In *IEEE CSDE 2020*, 2020.

[4] Morteza Alizadeh, Karl Andersson, and Olov Schelén. A survey of secure Internet of Things in relation to blockchain. *Journal of Internet Services and Information Security*, 3(10):47–75, 2020.

[5] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 375–392. IEEE, 2017.

[6] Damian Arellanes and Kung-Kiu Lau. Evaluating IoT service composition mechanisms for the scalability of IoT systems. *Future Generation Computer Systems*, 108:827–848, 2020.

[7] Kevin Ashton. That 'Internet of Things' thing. *RFID Journal*, 22(7):97–114, 2009.

[8] Ozalp Babaoglu, Moreno Marzolla, and Michele Tamburini. Design and implementation of a P2P cloud system. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pages 412–417, 2012.

[9] Juan Benet. IPFS-content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*, 2014.

[10] David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1):102397, 2021.

[11] Philip A Bernstein, Fausto Giunchiglia, Anastasios Kementsietsidis, John Mylopoulos, Luciano Serafini, and Ilya Zaihrayeu. Data management for Peer-to-Peer computing: A vision. 2002.

[12] Ranjita Bhagwan, Stefan Savage, and Geoffrey M Voelker. Understanding availability. In *International Workshop on Peer-to-Peer Systems*, pages 256–267. Springer, 2003.

[13] André B Bondi. Characteristics of scalability and their impact on performance. In *Proceedings of the 2nd International workshop on Software and Performance*, pages 195–203. ACM, 2000.

[14] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4:2292–2303, 2016.

[15] Shaveta Dargan and Munish Kumar. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, 143:113114, 2020.

[16] Ciprian Dobre, Florin Pop, and Valentin Cristea. New trends in large scale distributed systems simulation. *Journal of Algorithms & Computational Technology*, 5(2):221–257, 2011.

[17] Konstantinos Douzis, Stelios Sotiriadis, Euripides GM Petrakis, and Cristiana Amza. Modular and generic IoT management on the cloud. *Future Generation Computer Systems*, 78:369–378, 2018.

[18] Paul Dunphy and Fabien AP Petitcolas. A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, 16(4):20–29, 2018.

[19] Mohamed Elgharib, Mohit Mendiratta, Justus Thies, Matthias Niessner, Hans-Peter Seidel, Ayush Tewari, Vladislav Golyanik, and Christian Theobalt. Egocentric videoconferencing. *ACM Transactions on Graphics (TOG)*, 39(6):1–16, 2020.

[20] Ericsson. Cellular IoT in the 5G era. Whitepaper, 2020.

[21] Mojtaba Eskandari, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. Passban ids: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, 7(8):6882–6897, 2020.

[22] Ryan Farell. An analysis of the cryptocurrency industry. *University of Pennsylvania ScholarlyCommons*, 2015.

[23] Chunpeng Ge, Zhe Liu, and Liming Fang. A blockchain based decentralized data security mechanism for the Internet of Things. *Journal of Parallel and Distributed Computing*, 141:1–9, 2020.

[24] Michael Geller and Pramod Nair. 5G security innovation with Cisco, White paper. *Cisco Public*, pages 1–29, 2018.

[25] Zijiang Hao, Raymond Ji, and Qun Li. Fastpay: A secure fast payment method for Edge-IoT platforms using blockchain. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pages 410–415. IEEE, 2018.

[26] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.

[27] Shihab S Hazari and Qusay H Mahmoud. Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technology Letters*, 2(3):e100, 2019.

[28] Christine V Helliar, Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54:102136, 2020.

[29] J Baraković Husić, S Baraković, and A Veispahić. What factors influence the quality of experience for webrtc video calls? In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 428–433. IEEE, 2017.

[30] Muhammad Kazim and Shao Ying Zhu. A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications*, 6(3):109–113, 2015.

[31] Veton Kepuska and Gamal Bohouta. Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google home). In *2018 IEEE 8th annual computing and communication workshop and conference (CCWC)*, pages 99–103. IEEE, 2018.

[32] Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing bitcoin security and performance with strong consistency via collective signing. In *Proceedings of the 25th USENIX Security Symposium*, pages 279–296, 2016.

[33] Chakravanti Rajagopalachari Kothari. *Research methodology: Methods and techniques.* New Age International, 2004.

[34] Victoria L Lemieux. Blockchain and distributed ledgers as trusted recordkeeping systems: An archival theoretic evaluation framework. In *Future Technologies Conference (FTC)*, pages 1–11, 2017.

[35] Lulu Liang, Kai Zheng, Qiankun Sheng, and Xin Huang. A denial of service attack method for an IoT system. In *2016 8th international conference on Information Technology in Medicine and Education (ITME)*, pages 360–364. IEEE, 2016.

[36] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142, 2017.

[37] Petar Maymounkov and David Mazieres. Kademlia: A peer-to-peer information system based on the XOR metric. In *International Workshop on Peer-to-Peer Systems*, pages 53–65. Springer, 2002.

[38] William Metcalfe. Ethereum, smart contracts, DApps. In *Blockchain and Crypt Currency*, pages 77–93. Springer, Singapore, 2020.

[39] Manoranjan Mohanty and Waheeb Yaqub. Seamless authentication for online teaching and meeting. In *2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM)*, pages 120–124. IEEE, 2020.

[40] Arsalan Mosenia and Niraj K Jha. A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, 5(4):586–602, 2016.

[41] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. A brief survey of cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 745–752. IEEE, 2016.

[42] Edi Surya Negara, Achmad Nizar Hidayanto, Ria Andryani, and Rezki Syaputra. Survey of smart contract framework and its application. *Information*, 12(7):257, 2021.

[43] Kenneth Okereafor and Phil Manny. Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic. *International Journal in IT & Engineering*, 8(6):13–23, 2020.

[44] Maria Rita Palattella, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. Internet of Things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, 34(3):510–527, 2016.

[45] Jin Ho Park and Jong Hyuk Park. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8):164, 2017.

[46] Kriti Patidar and Swapnil Jain. Decentralized E-Voting portal using blockchain. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–4. IEEE, 2019.

[47] Dhiraj K. Pradhan and Sudhakar M. Reddy. A fault-tolerant communication architecture for distributed systems. *IEEE Transactions on Computers*, 31(09):863–870, 1982.

[48] S Subba Rao, Abraham Nahm, Zhengzhong Shi, Xiaodong Deng, and Ahmad Syamil. Artificial intelligence and expert systems applications in new product development—a survey. *Journal of Intelligent Manufacturing*, 10(3):231–244, 1999.

[49] Omar Said and Mehedi Masud. Towards Internet of Things: Survey and future vision. *International Journal of Computer Networks*, 5(1):1–17, 2013.

[50] Chayan Sarkar, SN Akshay Uttama Nambi, R Venkatesha Prasad, and Abdur Rahim. A scalable distributed architecture towards unifying IoT applications. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 508–513. IEEE, 2014.

[51] Meet Shah, Mohammedhasan Shaikh, Vishwajeet Mishra, and Grinal Tuscano. Decentralized cloud storage using blockchain. In *2020 4th International Conference on Trends in Electronics and Informatics*, pages 384–389. IEEE, 2020.

[52] Nidhi Sinha, Meenatchi Sundaram, and Abhijit Sinha. Authorization secured dynamic privileged escalation. In *2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, pages 110–117. IEEE, 2020.

[53] Ion Stoica, Robert Morris, David Karger, M Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for Internet applications. *ACM SIGCOMM Computer Communication Review*, 31(4):149–160, 2001.

[54] Antonio Tenorio Fornés, Samer Hassan, and Juan Pavón Mestras. Peer-to-Peer systems design trade-offs: a framework exploring the balance between blockchain and IPFS (unpublished). 2020.

[55] Feng Tian. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things. In *2017 International Conference on Service Systems and Service Management*, pages 1–6. IEEE, 2017.

[56] Anwar ul Haque, M Sayeed Ghani, and Tariq Mahmood. Decentralized transfer learning using blockchain & IPFS for deep learning. In *2020 International Conference on Information Networking (ICOIN)*, pages 170–177. IEEE, 2020.

[57] Jingdong Wang, Ting Zhang, Jingkuan Song, Nicu Sebe, and Heng Tao Shen. A survey on learning to hash. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(4):769–790, 2017.

[58] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7:22328–22370, 2019.

[59] Rebecca Yang, Ron Wakefield, Sainan Lyu, Sajani Jayasuriya, Fengling Han, Xun Yi, Xuechao Yang, Gayashan Amarasinghe, and Shiping Chen. Public and private blockchain in construction business process and information integration. *Automation in Construction*, 118:103276, 2020.

[60] Hyoeun Ye and Sejin Park. Reliable vehicle data storage using blockchain and IPFS. *Electronics*, 10(10):1130, 2021.

[61] Xueyun Zeng, Ninghua Hao, Junchen Zheng, and Xuening Xu. A consortium blockchain paradigm on Hyperledger-based Peer-to-Peer lending system. *China Communications*, 16(8):38–50, 2019.

[62] Shijie Zhang and Jong-Hyouk Lee. Analysis of the main consensus protocols of blockchain. *ICT Express*, 6(2):93–97, 2020.

[63] Shuai Zhang, Shufen Zhang, Xuebin Chen, and Xiuzhen Huo. Cloud computing research and development trend. In *2010 Second International Conference on Future Networks*, pages 93–97. IEEE, 2010.

Department of Computer Science, Electrical and Space Engineering
Division of Computer Science

ISSN 1402-1757
ISBN 978-91-7790-909-5 (print)
ISBN 978-91-7790-910-1 (pdf)

Luleå University of Technology 2021

FSC
www.fsc.org
MIX
Papper från
ansvarsfulla källor
FSC® C115359

SVANENMÄRKET
Miljömärkt trycksak
3041 0145

Print: Lenanders Grafiska, 139404

LULEÅ
UNIVERSITY
OF TECHNOLOGY