Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Blockchain Scalability: Data Engineering Solutions for Future-Proof Systems

[1]Divyeshkumar Vaghani, [2]Ketan Nandani, [3]Akram Chauhan
[1,2,3]Government engineering college, Rajkot

divyeshvaghani96@gmail.com
nandani.ketan@gmail.com
Akram.aic193@gmail.com

Article Info
Page Number: 278 - 301
Publication Issue:
Vol 68 No. 1 (2019)

Abstract

Blockchain technology has undergone significant evolution, transitioning through various stages from Blockchain 1.0 to the current developments aimed at version 5.0. Initially popularized by Bitcoin in 2009, Blockchain 1.0 introduced the concept of a decentralized digital currency, utilizing distributed ledger technology to facilitate transactions without a trusted intermediary. Despite its transformative impact on financial systems and organizational operations, including government and banking sectors, Blockchain 1.0 faces challenges such as high costs, long waiting times, and scalability issues. This research delves into the critical aspects of blockchain scalability, examining on-chain and off-chain solutions to enhance transaction throughput and efficiency. We explore various scalability solutions, including block size adjustments and block compression techniques, while also addressing the security and privacy concerns that arise in blockchain applications across diverse sectors like the Internet of Things (IoT) and healthcare. By analyzing existing literature and proposing future directions, this study aims to contribute to the ongoing discourse on improving blockchain systems to meet the growing demands of modern applications. Ultimately, our findings underscore the importance of innovative data engineering solutions in creating future-proof blockchain systems that can effectively handle increased transaction volumes while maintaining security and privacy.

Keywords: - Bitcoin, Blockchain technology, data engineering solutions, decentralized systems, off-chain solutions, on-chain solutions, scalability, smart contracts, transaction throughput.

Article History
Article Received: *09 September 2019*
Revised: *16 October 2019*
Accepted: *21 November 2019*
Publication: *28 December 2019*

I. Introduction

Blockchain is a shared record-keeping system that allows every user in a network to agree on the information without needing any outside help. Blockchain has become a groundbreaking technology because of its unique features like decentralization, permanence, transparency, and the ability to function without needing trust. This technology is being used to create applications in many different fields. Many studies use blockchain technology in different fields like finance, e-healthcare, the Internet of Things, supply chains, power management, insurance, and voting.

Blockchain technology started with Bitcoin (created by Nakamoto in 2008), and it works on a network where users can connect directly without needing a trusted payment system to help them. This type of decentralized system is very different from current business payment systems, and it changes how we trust security in those systems. Recently, many people in various fields like law, finance, and computer science have become very interested in blockchain. This is because it has important qualities such as being shared across many computers, not allowing changes after information is added, being secure, and protecting privacy (Abramaowicz, 2016).

But right now, the blockchain system has some problems with being able to handle more users or transactions.

1) Transactions take a lot of time to complete: "Tmall" is the best-known online shopping site in China. On November 11, "Tmall" made over 38 billion dollars in sales, with a high of 544000 orders being placed every second (Ifeng, 2019). In comparison, right now, Bitcoin can handle about seven transactions per second, while Ethereum can handle 30 transactions per second (Gervais et al., 2016). None of these blockchains can handle regular everyday transactions right now.

2) Long wait for confirmation: Since it takes about 10 minutes to create a Bitcoin block, it takes at least 10 minutes for a transaction to be confirmed. Because of the way the system can split, people usually wait 60 minutes to be sure a transaction is confirmed. Even the best Ethereum takes 18 seconds to finish confirming a transaction.

3) Expanding functions: Different situations have different people and needs, so it's hard to expect a blockchain system to handle all real-life applications. So, we need to connect the chains to prevent the blocks from being cut off from one another. This will help us achieve the true value of being interconnected.

The scalability problems can slow things down and make it hard for everyone to use blockchain technology widely. Several solutions have been suggested in the writings to address these problems.

On-chain scalability strategies (Rubin et al., 2014; Lombrozo et al., 2015; Cash, 2017; Jayarone & Wright, 2018) try to make blockchain systems better at handling more transactions. They do this by changing important parts of the blockchain, like how blocks are organized (Cash, 2017; Ding et al., 2019) or how transactions are structured (Rubin et al., 2014; Lombrozo et al., 2015). On the other hand, off-chain strategies (Poon & Dryja, 2016; Lin et al., 2020; Poon & Buterin, 2017; Mallaki et al., 2020) are made to handle transactions outside of the blockchain. This helps save storage space and reduces the work needed on the blockchain. For example, the Lightening Network and Raiden Network use this approach to make things better and faster.

This paper discusses how blockchain scalability can be enhanced through data engineering solutions for better future-proof systems.

II. Background

As mentioned earlier, blockchain technology has become a new way of using computers to help solve the trust issues that come with relying on a central authority. In a blockchain network, many computers work together to keep and secure a shared list of transaction records. They do this without needing to trust any single authority. Some special computers in the network, called miners, help add new blocks to a public record called the blockchain.

The first system was Bitcoin (created by Nakomoto in 2008), which let people send money (bitcoins) safely without needing a central authority to control it. In the blockchain network, miners gather transactions, solve tough math problems to agree on things, and then add those transactions as blocks to the blockchain. Since then, many platforms have been suggested for building on blockchain. These platforms let you use smart contracts, which are automated programs that can carry out actions and events on their own. Some examples are NXT, Ethereum, and Hyperledger Fabric.

We will explain how smart contracts work and talk about some blockchain platforms that help create them.

2.1 What is Blockchain Technology?

Blockchain technology is a system that allows many people to securely and openly record transactions without needing a central authority. It uses secure codes and a series of connected blocks to ensure that the recorded data is safe, cannot be changed, and everyone agrees on it. This removes the need for middlemen and builds trust in uses beyond just cryptocurrencies.

Blockchain technology is seen as a key force behind the "fourth Industrial Revolution," and it is easy to understand why (Kim, 2020). The idea of blockchain started back in 1976 with a paper about distributed ledgers in cryptography. However, it wasn't until 2008 that Satoshi Nakamoto, often called the "inventor of blockchain," published a paper explaining blockchain and how it could work without a central authority (Sarmah, 2018). It explained the problems with banking today and talked about how blockchain technology could solve them. This greatly changed how people could make transactions without needing a middleman. Since then, blockchain has been very important in improving many technologies and our world, and it is likely to continue doing so in the future.

Blockchain can do much more than just support cryptocurrencies (Marr, 2018). In supply chain management, companies are using blockchain to track where products come from and where they go. This helps make sure everything is clear, real, and done in a fair way. The diamond industry is using blockchain technology to check where diamonds come from and to make sure they are real. This helps reduce the sale of conflict diamonds. Healthcare systems are using blockchain to safely keep and share patient records while keeping them private. In the energy field, blockchain helps people trade energy directly with each other. For example, someone with solar panels can sell their extra energy straight to their neighbors. Also, governments are looking into using blockchain technology for safe voting systems. This could help stop cheating and encourage more people to take part in elections (Sam Daley, 2020). Estonia used blockchain technology in its online government system to provide safe digital identities and make public services work more smoothly (Karm, 2019). Blockchain impacts many areas, such as protecting intellectual property, decentralized finance (DeFi), and verifying art, where digital artworks are sold as non-fungible tokens (NFTs). These tokens are safe because of blockchain's secure design (Marr, 2018).

2.2 The Technical Side of Blockchain Technology

Blockchain technology has changed digital transactions by creating a safe and independent way to manage them (Atlam & Wills, 2018). It ensures that data is clear, trustworthy, and cannot be changed while also eliminating the need for middlemen (Atlam & Wills, 2018). The technology uses special codes to ensure that data is real and not tampered with, making it hard for hackers to interfere with the system (Yaga et al., 2018). Each block in the blockchain has a special code that connects it to the blocks before it, making it hard for anyone to change old transactions (Atlam & Wills, 2018).

This new technology provides a level of security that traditional methods do not have (Yaga et al., 2018). It allows quick transactions without needing middlemen, leading to faster processing times (Atlam & Wills, 2018). Using cryptographic methods in blockchain technology improves data safety and reduces risks for users. Technology's decentralized setup and secure coding have started a new time of trust and efficiency in different industries (Atlam & Wills, 2018).

One of the great things about blockchain technology is that it can create many new possibilities with smart contracts (Yli-Huumo et al., 2016). These agreements work automatically based on rules that are written in small pieces of code and run on the blockchain network. Smart contracts remove the need for middlemen and safely automate tasks that are saved in blocks on the blockchain. They provide benefits like being faster, more efficient, and more secure. This means transactions can be done reliably while also cutting down on costs from needing outside help.

Smart contracts can be used in many different areas, such as managing supply chains and transferring property. They offer endless chances to improve how businesses work in many different fields. However, using smart contracts can have problems, like not being able to handle a lot of users and some possible restrictions. It's important to look at how smart contracts affect how fast, effective, and secure transactions are while also thinking about the possible problems that might come up.

In summary, blockchain technology has changed online transactions by creating a safe and independent system. It makes sure that the data is clear, reliable, and cannot be changed, all without needing middlemen. Smart contracts are useful because they make things faster, save money, and are more secure (Yli-Huumo et al., 2016). Blockchain technology, with its basic ideas and new features, can change different industries and create new opportunities, like managing supply chains and transferring real estate, among other things. However, we need to think about the problems that might come up when putting this into action and any limits it could have.

The online world has changed a lot because of blockchain technology. It works on a system without central control, removing the need for middlemen and making transactions faster and safer (Atlam & Wills, 2018). The distributed ledger system carefully keeps track of every transaction, making sure everything is clear and stopping any changes to the data. Blockchain technology provides clearer information, stronger security, lower costs, and faster speeds.

Putting cryptographic algorithms into blockchain technology makes data safer and reduces risks (Yaga et al., 2018). The technology of connecting blocks using codes makes sure that the data is real and unchanged (Atlam & Wills, 2018). Each block has a digital signature made by mixing its information with the hash value of the block before it. This forms a chain that cannot be changed. These features offer an extremely high level of security, making it hard for criminals to trick the system.

Also, blockchain technology can change many industries, not just finance. Supply chain management can improve clarity and tracking, making sure that products are genuine (Marr, 2018). In healthcare, blockchain can safely keep and share patient records while keeping their information private. It can also help with smart contracts for buying and selling property and make things easier in areas like protecting ideas and inventions.

Even though blockchain technology has benefits, it also has problems like difficulty in growing and complicated rules. Scalability problems happen when handling a lot of transactions (Atlam & Wills, 2018). We need to create rules and laws that focus on how blockchain systems work, especially since they are decentralized and anonymous.

In summary, blockchain technology has changed how we make online transactions by offering a safe and shared system. It makes sure that data is clear, trustworthy, and cannot be changed, so there is no need for middlemen. Smart contracts are useful because they save time, lower costs, and keep things safe. Blockchain technology could change many industries, but there are problems like scaling up and complicated rules that need to be fixed. As blockchain technology grows and changes, it will keep altering how digital transactions and operations happen in many different industries.

2.3 Benefits of Blockchain Technology

Blockchain technology is becoming very important and is widely used for managing data in businesses. Budhi (2020) says that blockchain technology has some benefits, including being secure, allowing quicker transactions, being clear and open, not being able to be changed, and making it easy to track things instantly.

1] Clear and open communication

In blockchain, everyone can see all the transactions on a public record. Blockchain technology helps build trust and avoids confusion. It also lowers the chances of fraud, makes people more responsible, and improves how markets work. Using a distributed ledger, like blockchain, creates transparency, meaning anyone can see the transactions recorded on a network of devices. In normal systems, you can check information and data whenever you want because not all data is available to everyone. Also, they are controlled from one place and lack openness. Without clarity, users can track original transactions and can tell if fraud is occurring (Budhi, 2020).

2] Faster and Better Performance

How fast a transaction goes is really important because keeping customers happy is essential. Williams (2020) says that traditional non-digital methods take a long time, can easily cause mistakes to be made by people, and often require help from others. Blockchain technology can help complete transactions quickly and easily by automatically handling tasks. Blockchain can store information without paper. This makes it easier and faster to clear transactions because you do not need to combine many records while doing the transaction.

3] Immutability

Immutability means that once transactions are added to the blockchain, they cannot be changed or deleted. All transactions are verified and have the date from the blockchain, which creates a permanent record. This allows us to look up information over time, making blockchain a trustworthy source of data (Williams, 2020).

4] Safety

Once information is saved on a blockchain, it cannot be changed or removed. This unchanging nature keeps the information safe and secure, making it very hard to fake or change without permission. Blockchain uses strong security methods to keep transactions and data safe, making it hard for hackers and unauthorized people to get in.

The decentralized nature of blockchain means that there is no main place in charge. This lowers the chance of everything failing because of one problem or a main authority being attacked.

5] Quicker Transactions

Blockchain transactions happen fast because there are no middlemen, and everyone agrees on the details together. This efficiency is especially helpful for money transfers and payments between different countries. Blockchain networks work all day, every day, so people can make transactions anytime, even on weekends and holidays, without having to worry about regular bank hours. Smart contracts on blockchain platforms make transactions faster by automatically carrying out actions when certain conditions are met.

6] Immediate Tracking

All transactions on a blockchain are clearly logged in the order in which they happen. This visibility makes it easy to track items or products throughout the whole supply chain.

People in a blockchain network can see live updates on transactions and data, giving them immediate information about the condition and history of assets. Blockchain keeps a permanent record of all transactions that can be changed. This reliable history is useful for checking and confirming details, especially in areas like shipping and food safety.

Real Life Example

Blockchain is very helpful for the pharmaceutical industry because it improves privacy and helps companies follow global rules and laws. Blockchain helps keep patient health information safe and makes clinical trials happen faster (Arora, 2020).

2.4 Disadvantages of Blockchain Technology

Blockchain technology is becoming one of the most important new technologies today. Even though blockchain has many benefits compared to traditional systems, it still has some problems that need to be fixed. These problems include costs, speed, and privacy.

1] High Expenses

Blockchains cost a lot more than regular banks (Budhi, 2020). Team (2020) says that each transaction on the blockchain uses a lot of energy, which makes the average cost of a transaction between 75 and 160 US Dollars (Golosava & Romanovs, 2018). This shows that it's very expensive to run just one transaction, which is a big problem for businesses, especially new ones, that want to use blockchain in their operations.

2] Scalability and Speed

Blockchain transactions are very slow because of several reasons. One of these is how well something can grow or expand. The Team (2020) has stated that each block is set at a size of 1 MB, which restricts how many transactions each node can process (S, 2020).

This not only makes transactions slower, but it can also be hard to change a block after it has been recorded. This is because all the information and code in the blocks need to be rewritten. This takes a lot of time and can be expensive (Budhi, 2020).

Also, besides what was said before, blockchain does more tasks than a regular bank system, which makes transactions even slower. A blockchain has to perform several tasks, such as checking signatures, reaching agreements through methods like proof-of-work, and making sure everything is correct through backup checks. While all of this does help keep the blocks secure, it unfortunately makes transactions slower.

4] Not knowing enough about Blockchain and not Trusting it

Blockchain technology has only recently gained attention, especially since a significant change happened in 2014 (Sheldon, 2020). Since blockchain technology is still new, many people worldwide don't understand it yet. Because of this lack of understanding, they don't trust it and are hesitant to invest in it. Even though the future of blockchain looks promising, people feel safer sticking with traditional banking systems and regular encryption, which are more stable and trusted (Team, 2020).

5] Environmental Issues

Although blockchain technology is leading the way in many areas, its use of energy is still a big worry. Mining for cryptocurrencies, especially Bitcoin, uses a lot of energy and has been criticized for harming the environment (Budhi, 2020). The huge amount of computer power needed to solve complicated math problems and check transactions increases costs and also leads to a big carbon footprint. As the world pays more attention to being eco-friendly, we cannot ignore the environmental effects of blockchain technology.

6] Privacy and Security Problems

Even though people think blockchain is very secure, it can still be hacked. Transactions on a blockchain are usually described as unchangeable and safe because of encryption methods. However, problems can happen because of mistakes in how things are set up, errors in smart contracts, and tricks used by people (Sheldon, 2020). The openness of blockchain, which lets everyone see and check all transactions, could raise privacy issues when there is sensitive information that needs to be kept safe. Finding the right mix between being open and keeping things private is a constant struggle.

7] Regulatory and Legal Challenges

Blockchain technology works internationally, which can create challenges with rules and laws. Because many blockchain systems are decentralized and allow users to remain anonymous, it is hard to determine who is legally responsible when there are disagreements or fraudulent actions (Team D, 2020). Regulatory bodies around the world are still trying to figure out how to define and manage blockchain assets, initial coin offerings, and decentralized apps. This uncertainty can slow down the use of blockchain in industries that need clear laws.

8] Interoperability and Separation

The blockchain world has many different platforms and systems, each designed for various needs and industries. However, this division can make it difficult for different blockchains to work together easily. People are working on ways to make different systems work together, but it's still hard to make them compatible (S, 2020). Not having standard rules can lead to separate networks, making it hard to get the full advantages of a connected blockchain system.

In short, blockchain technology has some problems even though it is very successful today. There are some problems like high transaction costs, difficulties in growing and speeding up processes, not enough understanding, environmental issues from energy use, security risks, legal complications, and challenges with different systems not working well together. This shows that blockchain is still growing and changing. If it can fix its problems, it could completely change the technology world.

2.5 How Blockchain Technology Works

Blockchain technology is a new way to keep track of transactions using a shared network, which means no single person controls it. According to Putri et al. (2020), blockchain technology's qualities can create more reliable, trustworthy, secure, and efficient systems. Blockchain technology uses a quick, safe, and reliable way to carry out transactions, along with a system that spreads control among many users. This helps reduce rule-breaking because the information is available to everyone, and the way it is protected is very strong. Blockchain technology works by keeping a record of every transaction in a " lock." Each block includes details like the date, time, number of transactions, and other information. Every group of transactions made will be checked by the network, which means the users connected to it. After checking, transaction blocks will be added to the blockchain in a series that links them together. Each block in the blockchain will be coded using special technology to keep the information safe and stop anyone from changing it. The information on the blockchain is kept on many computers that are linked together, which means it isn't stored in just one place or by one organization.

Putri et al. (2020) assert that although blockchain technology was first used for digital money (like Bitcoin), it is now used for many other things beyond just cryptocurrency or money. This means that blockchain technology can be used in many areas like finance, accounting, banking, online shopping, health care, and education. According to Putri et al. (2020), because of blockchain technology, students can learn from different places at any time. This will definitely make any school or educational program work better by keeping track of student learning data, using secure blockchain records, reducing problems with losing information, and providing strong security. Blockchain

technology can help stop serious fraud, fake school records, and other problems in different industries that use its data. CPA Canada (2017) says that blockchain can help make financial reporting and auditing easier and more efficient. This can be shown through the checking of accounts, trial balances, journal entries, ledgers, and related spreadsheet files that auditors can access in different electronic and paper formats. So, planning an audit will take a lot of time.

Swan (2015) states that a blockchain is a public record that keeps track of every Bitcoin transaction made. Every 10 minutes, miners create a new block to update the blockchain with the newest transactions, helping it grow over time. So, blockchain helps Bitcoin users check their transactions quickly and correctly without needing banks or other financial organizations. In this case, each block added to the blockchain contains details about Bitcoin transactions that happen on the network. This information includes details like who sent the Bitcoin, who received it, how much was sent, and when the transaction happened. So, blockchain lets Bitcoin users check their transactions and see where their money goes clearly and correctly, without needing banks or other financial companies to help. Today, blockchain technology is used not just for tracking Bitcoin transactions but also for other things like storing data safely, creating digital identities, and speeding up secure money transfers outside of the Bitcoin system.

Based on Wilda & Harris (2020) The way a decentralized public blockchain works allows tourists to easily access transactions. These transactions can be shared widely so that everyone can see them. Rahardja et al. (2020) Using blockchain technology to make online shopping safer is very important.

When handling transactions with digital media, there are a few problems, like high fees for middlemen, slow payment processes, and risks related to security being controlled by a single source. Online shopping has its own way of keeping track of purchases, but it can be slow and costly at times. Swan (2015) asserts that Blockchain is like a new layer added to the internet that helps people make financial transactions, such as paying with digital money. Using this method, blockchain technology allows two people to make transactions directly between themselves without needing a middleman. Besides that, blockchain can also be used to create apps that check who people are, keep medical records safe, or run online voting.

2.6 Evolution of Blockchain

Blockchain technology keeps changing and improving over time in different stages to create various applications, as shown in the figure. Please provide the text you would like me to rewrite in simpler words. In each stage, Blockchain technology points out the different problems it has and suggests great solutions to fix them. The different stages of Blockchain development (from 1.0 to 4.0) are made to show different aspects, like what it can do, its features, strengths, challenges, and security problems. Version 5.0 is being worked on right now, and research teams are trying to make it better for various business needs. Figure 1 shows a summary of the different generations of blockchain, from 1.0 to 5.0, and outlines their uses, ways they agree on things, and important characteristics for each generation.

Blockchain 1.0

After that, the first use of Blockchain technology was a well-known cryptocurrency called Bitcoin, created by Satoshi Nakamoto in 2009. This was part of the first phase of Blockchain development, known as Blockchain 1.0. The idea of Bitcoin is well-known, and some of the most popular phrases about it online are "cryptocurrency," "cash for the internet," and "Internet of money." Bitcoin uses a system called distributed ledger technology to send money without needing a trusted middleman. This technology has quickly become a popular way to pay digitally and is used by many financial organizations around the world (Berentsen & Scha'r, 2016). Right now, Bitcoin is more than just a way to pay for things. It has also changed how economies work and how different organizations operate, like government departments, banks, and accounting firms. To keep transactions safe, Bitcoin uses a type of record-keeping that can be changed. This makes sure that all recorded transactions are accurate and that no one can alter them. Also, advanced security methods like hashing and digital signatures help keep users safe and their information private in the Blockchain system (Zyskind et al., 2015). Right now, Blockchain 1.0 has some problems, like high costs, long waiting times, and a lack of teamwork with other systems. These issues make it hard for more people to use it.

Blockchain 2.0

Blockchain technology is a fast-growing type of tech that is constantly getting better. It is changing how we create smart applications for people and businesses. Blockchain version 2.0 introduces smart contracts, which are small programs that run on the Ethereum Blockchain. These programs can perform automatic tasks and make decisions on their own (Delmolino et al., 2016). The main points of these programs are that they run on their own by following set rules and conditions, like time, how well something works, and certain decisions and checks (Idelberger et al., 2016). It is also important to say that these small programs (or contracts) work with users' identities to keep their personal information safe on the Blockchain network (Watanabe et al.). The benefit of smart contracts is that they might speed up the process of running and checking tasks without needing extra resources to do calculations. Additionally, it lets users clearly create smart contracts, which helps to avoid fraud and other risky issues (Cai & Zhu, 2016). In short, the Ethereum Blockchain is the main part of Blockchain version 2.0, where users can safely create and run smart contracts.

Blockchain 3.0

The main problems with earlier versions of blockchain (1.0 and 2.0) are that they mainly depend on the public Blockchain network and are not able to store a lot of data in the Blockchain's shared records. Bitcoin and Ethereum are available for everyone to use, and their information is created and saved on the blockchain every day. So, the main need is to keep a lot of data in different storage locations, like data servers and cloud storage (Khazraee et al., 2017). A new version of blockchain called Blockchain 3.0 has been suggested. This version uses the idea of decentralization to store a lot of data and to support different ways of legal communication. Decentralized applications use many servers to run their code, while a single server with little storage can only handle a few applications. The benefit of Blockchain 3.0 is that developers can write application code in any programming language. This is possible because it needs system calls to connect with the decentralized system to run the program. Besides the drawbacks, decentralized networks have several security issues, like ensuring who users are, giving them permission, and controlling who can access their data. Keeping users and their transactions private in a decentralized network is difficult, along with other security needs (Aitzhan & Svetinovic, 2016). To explain Blockchain 3.0, the creators of smart contracts made Genaro, which is the first public blockchain based on a Turing machine. It allows users to create and use smart contracts in decentralized storage systems, all in one location, with help from various network tools.

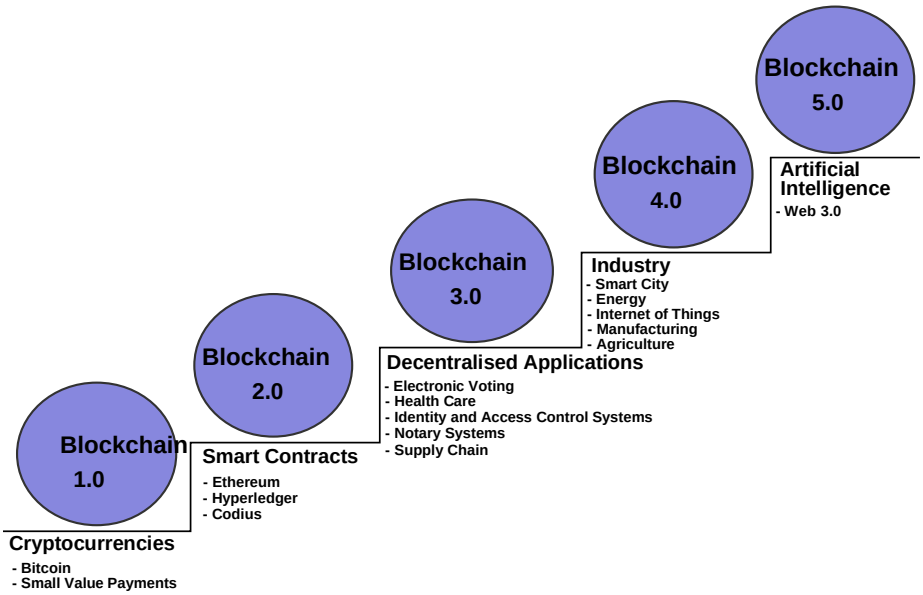

Figure 1: How Blockchain Has Changed Over Time

Blockchain 4.0

After successfully developing Blockchains 1.0 to 3.0, we now introduce Blockchain 4.0 to tackle the problems and limits faced in real-world use. Blockchain 4.0 is an updated version of Blockchain technology designed to bring it into the industry. Its goal is to make blockchain useful for creating and managing real-life applications safely and without a central authority. The new version allows us to suggest new solutions and connects the business world with the information technology field (Chung & Kim, 2016).

Also, Blockchain 4.0 helps businesses change how they work to be clear and trustworthy. It allows them to use reliable applications that keep track of everything on a secure and unchangeable system that isn't controlled by any one person. Industry 40 is a new and exciting technology that connects people and machines. It helps businesses grow and improves how well things work, which is good for people and the environment (Bodkhe et al., 2020).

The merging of Industry 4.0 and Blockchain 4.0 creates a new system based on reliable networks that remove the need for a middleman. Manual tasks are changed into connected systems using automated, independent systems that are supported by Blockchain technology. This coming together mainly focuses on using Blockchain technology like public records and shared databases. It also includes using smart contracts in businesses to get rid of paper contracts and to manage the network by agreement among users (Fernandez-Carames & Fraga-Lamas, 2019). Also, using Blockchain 4.0 in Industry 4.0 aims to make industrial processes clear from planning to execution and to connect industry rules with the basic features of Blockchain (Badzar, 2016).

Some examples of Industry 4.0 that have recently started using this new approach in their work include financial services, the Internet of Things (IoT), transport and logistics, smart grids, and eHealth.

Blockchain 5.0

Even though blockchain technology is still quite young, it has developed quickly. It is now used in many industries, like banking, healthcare, the Internet of Things (IoT), and managing supply chains. After doing well with previous versions, Blockchain 5.0 is made to meet the needs of future business people by organizing and making digital connections more official. So, it is very important to have Blockchain 5.0 in today's world. The goal of Blockchain 5.0 is to combine artificial intelligence (AI) and distributed ledger technology (DLT) to create a new type of decentralized Web 3.0 apps that focus on keeping data private, secure, and able to work well with other systems. By choosing this option, a project called "elictum Pro" is on track to succeed in the new era of Blockchain technology known as Blockchain 5.0. The "elictum Pro" Project uses advanced technology called Blockchain 5.0 to create virtual pathways on its special network. As a result, transfer speeds have greatly improved, and a new system was created that uses smaller blocks for quicker transactions.

2.7 Types of Blockchain

A public blockchain is a type of blockchain that anyone can use without needing permission. It works by using a method called a consensus algorithm, such as Proof of Work (PoW). Usually, the source code of a blockchain is available for everyone to see. This means people can change the code to create their own blockchain for making transactions. The biggest advantage of a public blockchain is that it could change how business transactions work today by removing middlemen. Additionally, you don't need special infrastructure to run the servers because of the decentralized nodes. However, a private blockchain does require its own legal setup. The official system limits people who want to join the network to carry out transactions. The advantages of this blockchain are lower transaction costs and fewer duplicate data. A consortium blockchain is a type of shared system used by a group of organizations. Only the companies in this group can check and confirm transactions. This blockchain is very useful for money and industry businesses.

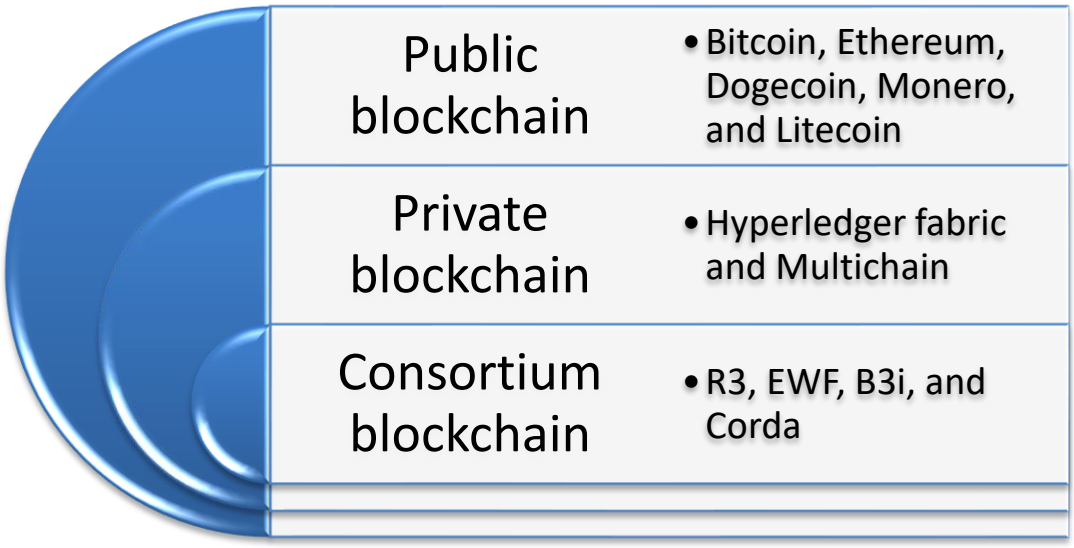

Figure 2: Types of Blockchain: Public, Private, and Consortium.

2.8 Reated Work

This part looks at different surveys that specifically study security and privacy problems in various applications that use Blockchain technology. We thoroughly compare current top studies about security and privacy in Blockchain-based Industry 4. 0 We look at different aspects like the year it was published, the publisher, the title of the paper, the applications discussed, the problems they address, the threats and weaknesses mentioned, the attacks identified, the techniques and solutions they suggest, and the future directions they propose.

The R3-Zcash group has released a report that looks at security and privacy issues on the blockchain. In this report, Yang et al. (2016), the paper looked at the security problems in blockchain, specifically focusing on keeping information safe and private in blockchain uses. The writers talked about basic threats to Blockchain services, like denial of service attacks and 51% attacks. They mentioned some solutions and suggested methods, like Hawk and Enigma, to help avoid these problems. This survey only pointed out a few security features and goals, along with their solutions, but didn't talk much about the latest weaknesses. Li et al. (2017) pointed out that Blockchain systems have issues with security and privacy. In this survey, the authors talked about the various weaknesses and attacks in these systems. Like the study by Yang et al. (2016), some security solutions like smart pool, Oyente, Towncrier, and Hawk are mentioned to tackle the basic security problems and privacy issues in Blockchain systems. However, these solutions only focus on using smart contracts to make sure the security rules of Blockchain systems are followed. Khalilov and Levi (2018) created a detailed study to tackle the issues of privacy and anonymity in digital cash systems that use blockchain technology. Bitcoin and its new digital money systems want to work with different groups to fix the problems of how addresses are shared in digital cash systems. The authors talked about the different attacks on these systems and suggested possible solutions. This study focuses on how safe and private financial transactions are using different methods. Joshi et al. (2018) conducted a survey to show the need for safety and privacy in some applications that use blockchain technology, like finance, healthcare, mobile services, defense, and the Internet of Things (IoT). The problem with this study is that the authors only looked at two types of attacks: denial of service and 51% attacks. They suggested using certain cryptographic methods to solve these issues.

Conti et al. (2018) explained the important security and privacy needs for Bitcoin and its related uses. This survey found and listed major weaknesses in the Bitcoin system, along with the threats they bring. It also grouped each threat and suggested solutions and methods to address them. The study looked at the major weaknesses in the Bitcoin system but mainly concentrated on the security needs and problems of the financial system. To address the privacy problems in Blockchain technology, a survey by Feng et al. (2018) showed how important it is to keep

personal information private and secure in finance apps. Additionally, this study discussed the few ways to protect against denial of service and Sybil attacks using cryptography.

Salman et al. (2018) explained how important different security services are, such as keeping information private, verifying identities, and controlling who can access information in areas like the Internet of Things (IoT), healthcare, and some cloud computing uses. The main issue with this study is that it only talks about security services and challenges for a few specific applications in blockchain. Dasgupta et al. (2019), different security services for various Blockchain-based applications, like big data, healthcare, and social networks, were explained. This research only showed the security needs and problems for important parts of privacy, and it mentioned a few encryption solutions.

Hassan et al. (2019) discussed the problems with privacy that come up when using IoT and Blockchain technologies to make services available to everyone. This survey looked at basic privacy features for safe communication in various Blockchain applications. This survey is an initial study about ways to protect privacy in IoT-based applications with a specific focus. The latest study by Zhang et al. (2019) looked at what is needed for security and privacy in cryptocurrency systems like Bitcoin. We talked about various security attacks on Blockchain services, like denial of service and mining attacks, along with different ways to protect against them. The main limitation of this research is that it only looked at the security and privacy needs related to financial transactions using different models.

In another study Wang et al. (2020), the authors talked about privacy problems that affect user identities and transaction details in Blockchain systems. This research looked at the usual ways to keep information safe and private. These methods include zero-knowledge proof, ring signatures, channel protocols, encryption, and coin mixing techniques like Mix coin, Blind coin, and coin join, all based on Blockchain technology. This study only looked at a few ways to protect privacy, focusing mostly on Blockchain technology. Casino et al. (2019) highlighted how important Blockchain technology is and how its features can be used in many real-world situations, from industry to business. This study was used in health care, the Internet of Things (IoT), voting, supply chains, and some business areas like managing data, banking, and insurance. However, this study did not talk about security risks and privacy problems in these Blockchain applications, and it also did not mention any ways to solve them. Akram et al. (2020) looked at all the security solutions made for Industry 4. 0 This study looked at only a few security methods that use blockchain. It talked about the good and bad sides of these methods and mentioned the problems with working together and managing them.

In another study, Maesa and Mori (2020) examined how blockchain can be used in Industry 3. 0 and its connections to different applications. They talked more about the issues and what is needed to use Blockchain in Industry 3.0. This study had a limitation because it only looked at how important Blockchain technology is for Industry 3.0 and didn't address the need for security and privacy concerns. Mohanta et al. (2019), the writer talked about how important blockchain is for many uses, like in healthcare, finance, the Internet of Things (IoT), cloud computing, power grids, and smart transportation. They also pointed out the various security and privacy problems and challenges that come with these applications. The problem with this survey study was that it only talked about security and privacy issues and did not mention any solutions to fix those problems. In a recent survey by Perera et al. (2020), researchers looked into using Blockchain technology in Industry 3.0, especially in the construction field, by showing how it could be useful in different ways. This study only looked at the different parts and features of blockchain in industry. It did not go into detail about the security problems or risks related to these applications or how to address them.

Fernandez-Carames and Fraga-Lamas (2019) studied the pros and cons of using blockchain and smart contracts to create applications in Industry 4.0. This study mainly aimed to show a simple guide for Industry 4.0 researchers on how to use blockchain to make industries safer from cyber threats. Bodkhe et al. (2020) carried out a survey to look into new Blockchain solutions and how they can be used in different smart applications, particularly in Industry 4.0. This study only looked at the good and bad points of the solutions we have, along with a few ways to improve them. Also, this study did not explain much about security risks and privacy issues in blockchain uses.

The Industry 4.0 revolution has changed how factories work. One example is Cyber-Physical Production Systems (CPPSs), which can offer many benefits and future possibilities, like being aware of themselves, predicting what will happen, and changing themselves when needed. CPPSs try to link virtual and real production, but we need a combined computer system to make these systems work in the real world. To do this, Lee et al. (2019), researchers looked into how using blockchain in real-life systems that combine physical and digital elements could affect the way we create and use these systems. Also, a three-layer Blockchain system was created to help industrial researchers understand how Blockchain technology will be used in future manufacturing. To keep devices and networks safe and private in smart factories, Lin et al. (2018) introduced a system that uses blockchain to securely confirm identities and manage detailed access rules.

Business process management (BPM) works with Industry 4.0 and Blockchain technology to make business operations easier and more trustworthy. It uses features like decentralization (no single control), immutability (data cannot be changed), and accountability (responsibility for actions) to digitize and automate workflows. This helps different service providers work together better and ensures that assets are reliable. To achieve this goal, Viriyasitavat et al. (2018), a study looked into a way of managing business processes for services that combine different offerings. It uses blockchain technology to find the best partnerships and check if businesses can be trusted, all through automated management tools.

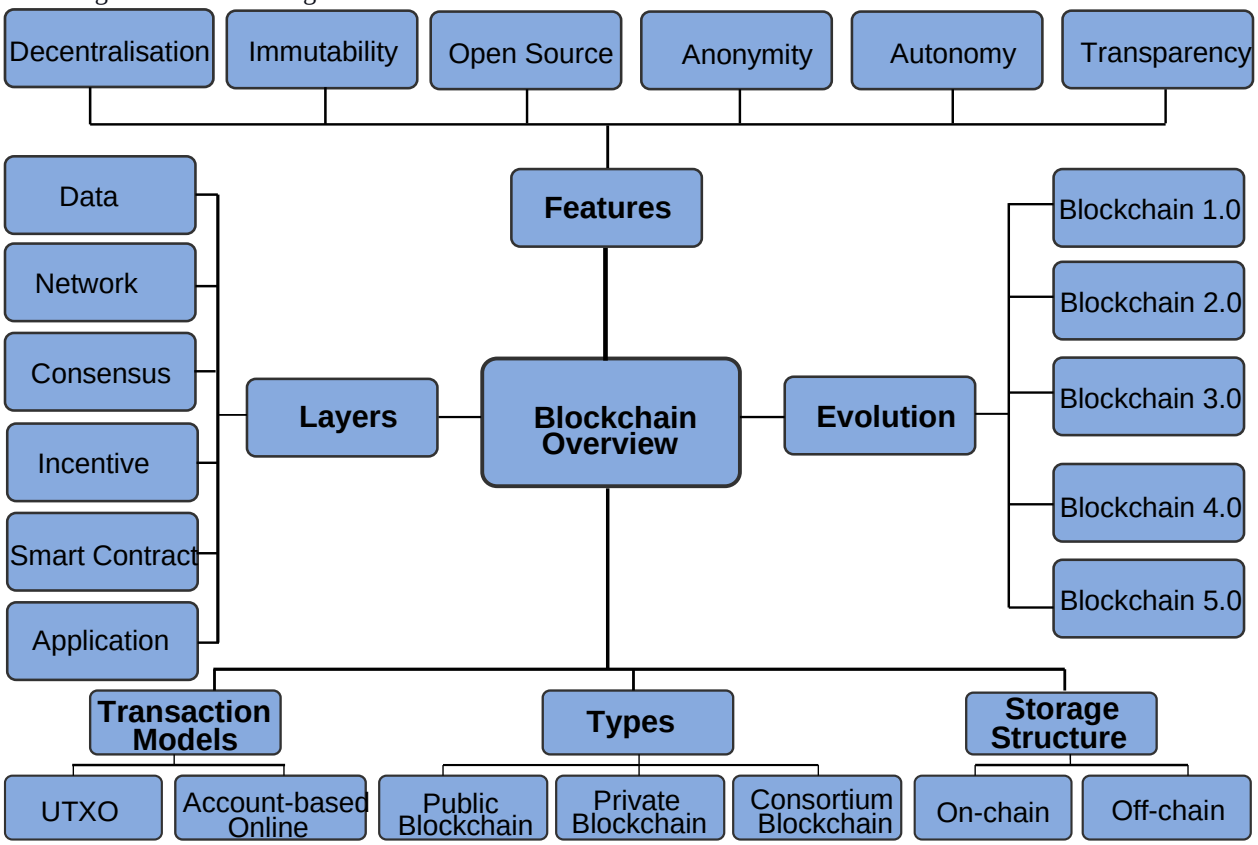

Figure 3: A Generalised Overview of Blockchain

2.9 Using Blockchain Technology in Different Areas

Blockchain technology is a new way to solve data security issues in different industries. In finance, blockchain can help make transactions faster and better. It keeps transactions and data safe and reliable, and it can lower other costs, too. In different areas, blockchain technology can be used to create digital money like Bitcoin. Also, blockchain technology can be used in different industries like logistics and supply chains. It helps keep track of items, improves how goods are delivered, and makes the whole supply chain more open and responsible.

Blockchain is a way to keep track of transactions online without needing help from banks or governments. Based on the work of Suprayitno and Cempaka Timur (2020), Blockchains offer both possibilities and problems when used to improve emergency decision-making systems by reducing risks from relying too much on one source. Blockchain technology provides strong proof that it helps people make good decisions. Also, blockchain can make the network used for making quick decisions in emergencies much stronger and more resilient. The idea of being antifragile means getting stronger when it faces challenges or problems. So, the more people or machines try to break it, the tougher it becomes. Blockchain technology improves functions by providing a reliable version of information, making data unchangeable, and allowing processes to run automatically. Bringing together blockchain technology and machine learning will help different groups work together better, improve over time, handle future challenges more effectively, and maybe even predict potential issues before they happen. According to Suprayitno and Cempaka Timur (2020), Blockchain technology can help keep networks and big systems working well while making decisions during emergencies and disasters. Blockchain technology can be set up to find, separate, and reduce attacks that target a weak spot in any network. Based on the work of Suprayitno and Cempaka Timur (2020), Blockchain technology helps build trust in buying and selling by allowing better visibility and teamwork between where products come from and where they go. Companies that rely on supply chains all over the world are starting to use blockchain technology. Blockchain technology can help modernize the supply chains for defense by connecting the real world with the digital world. It can create a system for logistics that focuses on teamwork and trust.

As stated by Princess et al. (2020), Blockchain technology is a quick, safe, and clear way to do transactions. It has a strong system for keeping control that makes it hard to break into. This is because the information is open for everyone to see, and the security method is very tough to bypass. Blockchain technology is a useful tool for fixing problems in online education, like keeping data safe. This technology is usually used in finance, online services, and connected devices. Also, companies in the industrial sector are using blockchain technology for product design. Paulus et al. (2020) Blockchain is a safe and reliable way to record transactions online without a central authority. In this situation, blockchain helps make things clearer and more responsible while also making transactions faster and safer. Blockchain systems make data safer by lowering the chances of changes or cheating. Also, the transaction process gets quicker and easier since there are no middlemen involved, which helps save money and time. Using blockchain helps people benefit from reliable and safe modern technology. As stated by Paulus et al. from Indonesian Christian University, one thing that makes blockchain different from other technologies is that it has a shared record that keeps track of transactions between people. This lets many writers add notes about transactions, making it easier for everyone to record them without being in one central place. In this situation, people do not need to trust each other because the transactions are written down clearly and can be seen by everyone. Also, the blockchain system helps keep safe and clear records, letting users check transactions on their own without needing to trust others. Blockchain is very secure, so the recorded transactions cannot be changed or messed with by anyone.

2.10 Using Blockchain Technology

Blockchain is a way to keep track of transactions online without needing help from banks or governments. So far, the main advantage of blockchain technology has been to keep cryptocurrency transactions safe, like those for Bitcoin and other types of digital money or assets. Triantonno (2020) says that blockchain has a big impact on new technology in accounting. Fraud accounting is a type of accounting that uses blockchain technology to help stop cheating in financial records. Larasati (2017) talks about how combining efforts to prevent fraud is affected by internal controls, a whistleblowing system, and good corporate governance. This means that if blockchain is used to stop accounting fraud, it needs to change these three things: changing financial statements, pretending to be someone else, or hiding accounts.

Khaerunisa and Enjat Munajat (2020) stated that Blockchain technology could change accounting practices to make them faster and more efficient. Blockchain is a system that is not controlled by any one person or group. It allows people to share information directly with each other. It keeps information safe using special codes, is permanent, and works through digital programming. According to Augusta et al., blockchain is a growing record (database) made up

of blocks that are linked together and protected using special codes. A block has two main parts: the head and the body. The header has the hash of the last block, the time the block was made, and the nonce. At the same time, the block has a list of transactions saved. A block is like a package that holds details about transactions and extra information to keep the data safe and accurate. According to Augusta et al. (2020) blockchain technology means that an organization does not have to depend on one server. Instead, all data is shared across the whole network. This helps prevent changes or additions to the data without everyone's agreement, keeps the system running even if one part fails, and protects user accounts from hacking. Blockchain technology helps keep data safe, which makes it great for storing information that could be changed or tampered with. Blockchain can help keep students' identities safe, protect their privacy, and secure their data. As mentioned earlier, blockchain data is permanent and cannot be altered. Blockchain can make things easier by keeping track of digital certificates, managing intellectual property, checking diplomas, and making fast and reliable monthly money payments. Blockchain helps prevent students from changing their grades, majors, and certificates. This makes it easier for employers to check that job applicants have the right skills for the job. In simple terms, blockchain technology is a system that keeps records in many places at once. It can make students' academic records clearer and more open for everyone to see.

Firmanto (2019) explains that blockchain is a tool that businesses can use to keep track of the money coming in and going out of different parts of their organization without any limits. Blockchain helps create strong trust between company leaders and outside parties like investors, the Indonesian Financial Exchange (IDX), the Financial Services Authority (OJK), Bank Indonesia (BI), internal auditors, external auditors, and other groups connected to the company. Companies can use blockchain to help stop accounting fraud.

According to Sansone et al. (2020), blockchain allows people, charities, and local groups to give donations directly without needing to use many middlemen. This can lower the costs and time needed to make transactions while allowing for very thorough checks of donation details. Donations made on the blockchain are kept on a public list that anyone can see and verify. In this situation, it is very clear and honest because donors can see exactly where their money goes and make sure it really reaches the right people. This way, blockchain can help people trust the institutions and organizations that handle donations more. Li and Chen (2020) say that Blockchain technology has three key advantages for making supply chains stronger. First, blockchain makes it easier for businesses in the supply chain to share information with each other. It is really important to make sure that the information shared is right and trustworthy. Second, blockchain technology helps keep track of information very accurately. This makes it easier for users to see where products come from, what their condition is, and the status of shipments. Finally, blockchain helps build trust and teamwork among people involved in the supply chain. Using blockchain in supply chains can make things work better and clearer while also building trust among everyone involved.

III. Scalability Issue

Blockchain technology can only handle a certain number of transactions at one time. The number of transactions a blockchain can handle relies on how big each block is and how long it takes to create them. When a lot of transactions occur at the same time, it takes longer to add new blocks, which can cause delays and increase transaction costs. This blockchain transaction also needs a pretty high fee to go through. These costs can be an issue in areas like farming or small businesses that don't make a lot of money. Blockchain is a new technology that is still being worked on. Many people and organizations still don't understand how to use blockchain well in different areas, and it might take a while for everyone to get used to this technology (Utomo, 2020). These problems will always be there as blockchain technology keeps growing and being used in different areas. With some work to find the best answers, blockchain technology can get past these problems and offer great advantages for different industries and society in general.

As blockchain systems keep growing, scalability is becoming a big problem and a major obstacle to using blockchain widely. Blockchain is a system where everyone involved keeps a copy of the same data and checks each transaction together. As more people join the network, it takes longer to agree on each transaction. As a result, delays go up, and the system works less effectively. Also, as the blockchain gets bigger, full nodes need more

storage space to save the data and more internet speed to download all the data when they are first set up. In this survey, we have sorted scalability solutions into five groups:

- On-chain scalability
- Off-chain scalability
- Scalable consensus mechanisms
- Directed Acrylic Graph (DAG)-based scalability
- Horizontal scalability through sharding

Figure 3 shows the different groups of categories and the solutions available in each group that we talked about in this paper. Each type of scalability solution can alter different parts of the blockchain setup. In the next sections, we will give a clear overview of the current ways to improve scalability. At the same time, these solutions are looked at based on how well they can grow and perform. This includes measuring things like speed, delay, storage space, and data transfer capacity.

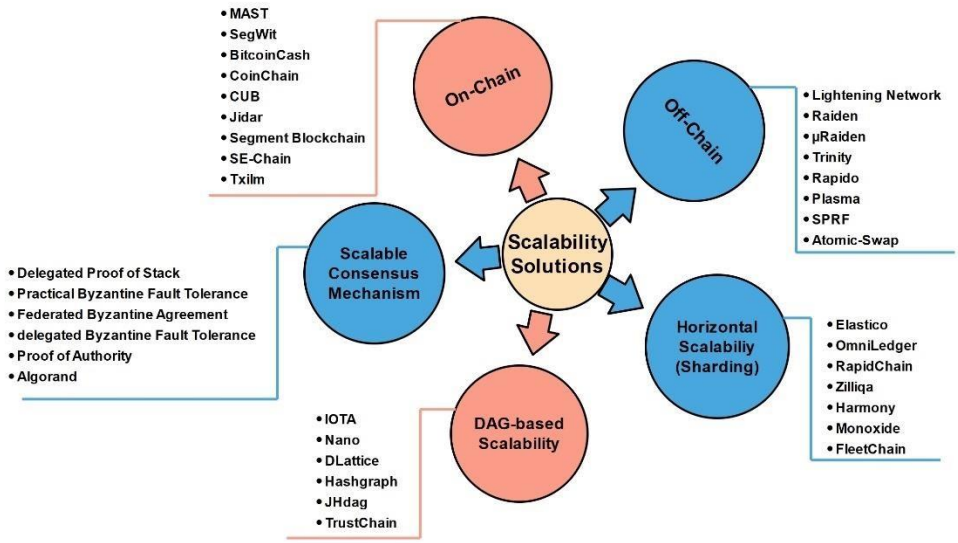

Figure 4: Taxonomy of scalability solutions.

1. **On-Chain Scalability Solutions**

On-chain scalability solutions are ways to change important parts of the data system in blockchain design to make it work better. The data layer part of this paper says that important parts of the data layer are blocks, transactions, Merkle trees, digital signatures, and hash functions.

For example, some studies (Cash, 2017; Garzik, 2015) use a method where the block size is made bigger. The bigger block method allows more transactions to be processed at once because larger blocks can hold more transactions. This means that when a block is added to the blockchain, more transactions get confirmed. However, using larger blocks can make it take longer for them to be shared across the network.

Also, block compression is a technique used by some studies (Yu et al., 2020; Nadiya et al., 2018) to reduce the amount of space the blockchain takes up and to help the network use less data. In this part, we will look at some key solutions to help improve how on-chain systems can handle more transactions.

i) Merkelized Abstract Syntax Tree (MAST)

The Merkelized Abstract Syntax Tree (MAST) is a proposal from Rubin and others in 2014 to make Bitcoin better. It aims to help Bitcoin handle more transactions by improving how Bitcoin scripts work. To achieve this, it uses ideas from the Merkle Tree and Abstract Syntax Tree (AST) to show the parts of Bitcoin transactions in a clear and safe way. In Bitcoin, transaction outputs have a locking script called "encumbrance." This script outlines the rules

that say how the recipient can use that output. The AST is a tree that shows the main structure of a computer program's code in a simple, organized way. So, by using AST, MAST can keep the more complicated locking scripts in a Merkle tree format and get rid of parts of a script that are not needed for the transaction. So, MAST uses both the Merkle tree and AST to ensure that the data is safe and to save space when recording transactions. In summary, MAST leads to smaller transactions and better privacy, and it allows for bigger smart contracts. However, it also makes the contracts involving Bitcoin more complicated.

ii) Segregated Witness

Segregated Witness (Segwit) (Lombrozo et al., 2015) is a change to Bitcoin that helps it handle more transactions. It makes block space available so that more transactions can fit in each block, which speeds up how quickly transactions are confirmed.

Bitcoin transactions have three main parts: inputs, outputs, and witness data. Inputs show where the money is coming from, outputs show where the money is going, and witness data includes a signature and a script to confirm the transaction is valid. To create more space on the block, Segwit takes the witness data out of Bitcoin transactions and keeps it in a separate block instead of on the main blockchain. Since witness data takes up about 70% of the block size, getting rid of it allows Segwit to handle 1.7 to 4 times more transactions than Bitcoin. This leads to lower transaction fees (Kim et al., 2018).

Segwit also wants to stop changes to Bitcoin transactions. Malleability is when attackers can change the transaction ID of a transaction by altering its digital signature, but the data remains the same as before. They then send this modified transaction back into the network, making other users believe that the original transaction has not been confirmed (Decker & Wattenhofer, 2014). Besides fixing problems with scaling and changing transactions, Segwit helps create solutions that work outside the main blockchain (for example, The Lightning Network (created by Poon and Dryja in 2016) will be talked about in the next sections. It is now being used by Litecoin (according to Reed, 2017). Despite its benefits, the main downside of Segwit is that, since it is a soft fork, it can cause a fungibility issue. This happens because not all nodes in the network have to update from the older version of Bitcoin. Also, Segwit uses a lot more resources, such as space and internet speed, because it can handle more transactions at once. Also, using Segwit is difficult because it makes the code more complicated.

iii) Bitcoin Cash

Unlike Segwit, which is a kind of update, Bitcoin Cash (Cash, 2017; Javarone & Wright, 2018) is a hard fork of Bitcoin. This means it divides the Bitcoin network into two separate blockchains. To make it easier for more people to use, Segwit works to make transactions smaller, while Bitcoin Cash aims to make the blocks bigger. BitcoinCash changes the original Bitcoin code to make the block size limit bigger, from 1 MB to 8 MB. This allows for more transactions to be processed at once, averaging 116 transactions every second. As a result, Bitcoin Cash allows transactions to happen faster than Bitcoin. However, it sacrifices some decentralization because there are fewer nodes that can handle or share the bigger blocks. In simple terms, it needs more computing power and internet speed.

iv) CoinChain

CoinChain (Chan et al., 2020) is a flexible and removable blockchain that protects privacy and serves as a sidechain for Bitcoin. The coin chain can easily grow in size for storage and the blockchain, but it processes transactions at the same speed as Bitcoin. Privacy issues make it hard to have anonymous transactions and keep the sender, receiver, and transaction amount confidential. These concerns complicate current cryptocurrencies and limit their ability to reduce or simplify blockchain data. In contrast, CoinChain is an easy-to-use system that works like handing over cash. It uses special codes for different amounts of money, which users exchange with each other. Each coin has a special CoinID, and people move ownership of coins by making transactions. So, you can simplify the blockchain by only keeping track of who last owned the coins. However, there are some problems with CoinChain. First, you cannot make partial payments. Second, users need to use or mix all the coins they initially put in to maintain their privacy. Third, in CoinChain, checking for things like money laundering or tax evasion can only happen if all transaction details are openly shared.

v) Storage Efficient Solutions

Using too much storage is a big problem that keeps many devices from joining the blockchain because they don't have enough space. In this part, we will talk about some projects that aim to improve storage efficiency in blockchain.

CUB (Xu et al., 2018) helps save space by breaking the whole network into smaller parts called "consensus units." In these units, the nodes work together to keep one copy of the blockchain instead of each node having its own separate copy. So, it helps save storage space for people in the blockchain network. Also, CUB offers ways to improve how blocks are assigned and reduce the cost of queries. The main problem with CUB is that it depends on a strong trust assumption that is difficult to meet in real life.

Jidar (Dai et al., 2019) is a way to reduce data for Bitcoin that does not require trust. In this system, each node only needs to keep the transactions that matter to it and some parts of the Merkle tree from the entire block that is necessary to check new transactions. Jidar can lower the storage cost for each node by around 1.03% compared to the regular Bitcoin system. The problem with Jidar is that it does not work with regular smart contracts.

Also, if some nodes need an entire block, they have to ask different nodes for the bits of that block's data. After getting all the bits, they put them together to form the complete block. However, this process needs a reward system to work effectively.

Segment blockchain (Xu & Huang, 2020) is a way to store blockchain data using less space. The main idea of the Segment blockchain system is that it divides the blockchain into smaller parts called segments. Each node only keeps one segment instead of the entire blockchain. It has been shown that Segment blockchain uses much less space for storage while still keeping the blockchain safe and decentralized. Also, Segment blockchain helps with blockchain sharding by keeping transaction checking and storage apart. On the negative side, it is only good for uses that do not require a lot of transaction results. SE-Chain (Jia et al., 2020) is a type of blockchain system that can easily grow to handle more storage. In the SE-Chain framework, each transaction is saved in a special tree called the Adaptive Balanced Merkle tree (AB-M tree). The full nodes keep a portion of the blockchain-based on a set rule about how much to save. Also, to keep the stored data safe on the full nodes, a way to check how reliable a node is has been suggested. Another benefit of SEChain is that it helps to find data quickly and easily with the AB-M tree.

vi) Block compression

Some studies have used block compression to reduce the amount of data sent over the network, which is important for improving how well blockchains can grow.

One solution is Txilm (Poon & Dryja, 2016), where each block has a short summary of the transactions instead of the full details of the transactions. To create a compact version of a transaction, the transaction is processed twice with a special method called hashing. First, it uses SHA256, which gives a 256-bit code known as TXID. Then, it uses another hashing method. CRC32, CRC4p, and CRC64 are methods that create a short code called TXID-HASH, which is a fixed size of bits. So, the final result, which is TXID-HASH, is a short way to show a transaction that is added to a block along with the TXID-HASHes of other transactions and the block header. The block header also includes a SHA256 Merkle root, which is a summary of all the included TXIDs. After that, the user sends the compact block through the network. When the full nodes get the compact block, they need to look in their memory pool to find a transaction ID (TXID) that matches each TXID-HASH in the compact block. If we find one matching TXID, we will accept the TXID-HASH. If not, the full node asks the sender or other nodes for the missing TXID. Also, when there are multiple matches for a TXID-HASH, the issue of hash collisions is fixed using the Merkle root. In conclusion, Txilm reduces data by 80 times, which greatly saves network space and makes the blockchain work faster.

IV. Future Directions And Unresolved Questions

Many studies have looked into problems with scaling up recently, but there are still some issues that weren't fully figured out and need more work in the future. In this part, we talk about the problems that are still not solved and the future research areas for each type of scalability solution.

Q. On-Chain Scalability

Secure blockchain pruning: A big blockchain takes up too much space, which can cause centralization issues because there is not enough storage. One way to make the blockchain smaller is to get rid of unnecessary and outdated information. This helps save storage space on the computers that hold the blockchain. Many studies (Reddy, 2020) have looked at blockchain pruning recently, but there is still an important question to answer: What data can be deleted at what times without putting security at risk?

Blockchain data query: Because blockchain data is decentralized and spread out, it can be hard to get the specific information you need. As the blockchain gets bigger, handling different types of requests, like single searches, range searches, and condition checks on a lot of data, faces problems with speed and network capacity. So, finding a good way to search for data on the blockchain is a problem that hasn't been looked at enough in written research.

R. Off-Chain Scalability

Future work can focus on using off-chain blockchains to explore more ways to do calculations outside the main chain and create systems that combine on-chain and off-chain processing.

S. Scalable Consensus Mechanisms

New proof-based agreement methods: Most of the ways to agree on things in a scalable way are based on voting, but there aren't any proof-based methods that are scalable. So, we need to study how to create safe and quick proof-based algorithms more. One idea is to create rules that use non-negotiable rewards like reputation or being well-known, where the difficulty of mining can be adjusted as needed.

Multi-block consensus methods: Changing how agreement protocols work so they can agree on several blocks at once can significantly increase the amount of work done.

T. DAG-Based Scalability

Trade-off: Current systems that use DAGs to manage or balance different factors well. For example, IOTA (Divya & Biradar, 2018) and GraphChain (Boyen et al., 2018) improve speed and ability to grow, but this comes at the cost of security and reliability. On the other hand, some data ledgers that use DAGs, for example, Prism (Bagaria et al., 2019) and OHIE (Yu et al., 2020), ensure data is always consistent, but this can make them slower and less able to handle large workloads. So, creating a solution based on a DAG that can balance different measurements is still a difficult problem.

Helping with off-chain transactions: Changing DAG-based systems to better support off-chain transactions is a promising area for future development. This approach can benefit from both off-chain methods and DAG-based systems.

System setup: The setup instructions outline all the important requirements that each participating node needs to have ready at the start of the protocol. Some current systems that use DAG (Directed Acyclic Graph) depend on a starting block called a genesis block. Meanwhile, other systems set up several parallel chains at the same time, but it's not clear how these parallel chain setups work. So, using a new and clear system design could be looked at as something to work on in the future.

U. Horizontal Scalability Through Sharding

Cross-shard transaction: Cross-shard transactions create a lot of extra communication and can slow down the system, making transactions take longer to confirm. So, finding a way to divide transactions into different groups while keeping cross-group transactions low is still a problem that hasn't been solved. In this context, the authors (Nguyen et al., 2019) suggested a new way to divide work called OptChain, which helps to place transactions in the best way. Also, a new permissioned blockchain called "Sharper" has been introduced in a study by (Amiri et al., 2020). It improves transaction processing by grouping network nodes into clusters. Sharper uses two decentralized methods to make cross-shard transactions work better. We still need better ways to handle transactions between different sections to make them faster.

Resharding: The resharding process is difficult for blockchains that use sharding because it requires rearranging the network, resulting in a large amount of data being moved. SSChain (Chen et al., 2019) is the first public blockchain that offers complete sharding without needing to rearrange or move data.

Adaptable harmful attackers: The resharding process is done to stop bad users from taking control of a shard by ruining the members of that shard during certain time periods of the protocol. It is important to protect committee members from attackers who adapt slowly as well as those who adapt quickly.

A good idea is to use sharding along with machine learning to study how users act on the network and find harmful users.

The Future of Blockchain

The Gartner Hype Cycle for Emerging Technologies 2017, shown in Figure 2 below, says that blockchain is still in the "Peak of Inflated Expectations" phase. It is expected to level off in "five to ten years." however, this technology is seen as getting worse as it enters the stage called the "Thought of Disillusionment." because more people are using blockchain for different purposes beyond just cryptocurrency, the authors of this paper predict that it will take about "two to five years" "instead of "five to ten years" for it to fully develop. Blockchain can really help people in developing countries if it is used widely in online government services. It can be used for things like managing identities, transferring ownership of valuable items like gold, silver, and diamonds, healthcare and other business activities, and helping people access financial services. However, this will really depend on the choices made by the country's leaders.

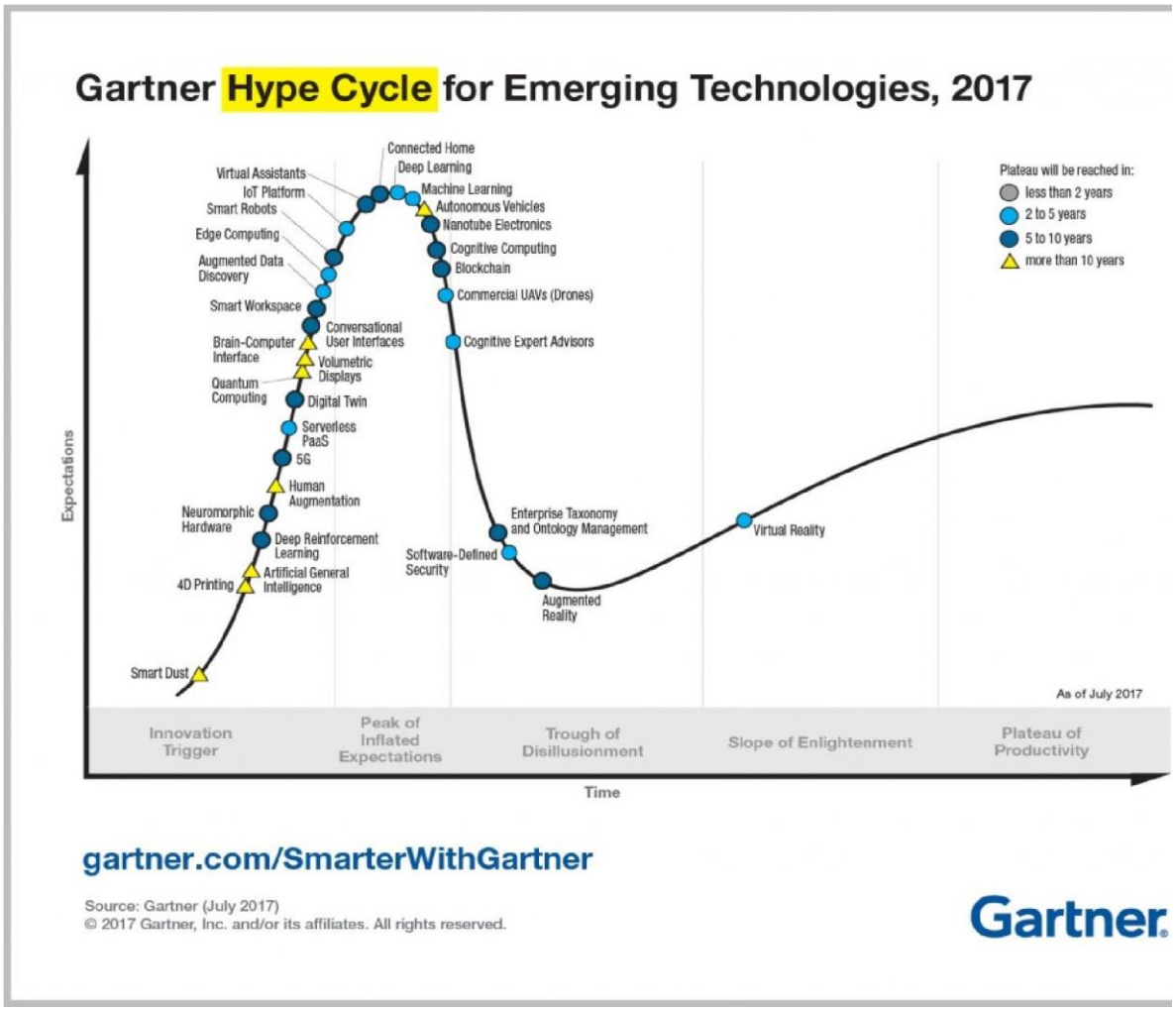

Figure 5: Gartner Hype Cycle, 2017 (Gartner, 2017)

The future safety of digital data using blockchain technology

Keeping digital information safe is a big problem in today's world (Johnson et al., 2020). Threats like cyberattacks, hacking, and identity theft are getting more complicated. So, it is important to find good ways to protect our online information. One hopeful solution is blockchain technology. Blockchain technology is a system made up of linked blocks, and each block holds information or transactions. What makes blockchain technology special is how safe and clear it is. Information saved in the blockchain cannot be changed and is kept forever. The agreement used in blockchain makes it hard for bad people to change or remove information that is already there. Using blockchain technology for digital data security in the future offers key advantages (Davis et al., 2020). First, blockchain is very secure because it uses tough coding methods. The information saved in the blockchain is locked and can only be accessed by approved people. Second, blockchain provides clear and trustworthy information.

Every time something happens or data changes, it is noted down, and everyone involved can see it. This helps lower the chances of changing or faking the data.

Also, the blockchain can automatically check and confirm data (Wilson et al., 2020). Using smart contracts allows business rules and security measures to be followed automatically. This means less reliance on other people and improved efficiency. Blockchain technology can help keep information safe in different areas like health care, finance, and shipping. There are some problems to solve when using blockchain technology to keep digital data safe in the future. These problems include making it work for lots of users, protecting privacy, and needing powerful computers. To solve this problem, we keep doing research and development.

V. Conclusion

In summary, blockchain can grow and become a key way to manage data in our society. Blockchain is important for cryptocurrency because it helps keep a safe and independent record of transactions (Hayes, 2020). Blockchain technology is a special type of record-keeping system that is shared by many people and cannot be easily changed. It consists of a series of blocks, and each block holds a group of information. The blocks are connected using secure methods and a series of information linked together (A. S, 2020).

Blockchain has a big effect, leading us to a future that uses data more. The growing promise of blockchain technology has some challenges: blockchains are often much more costly than traditional banking systems (Budhi, 2020). According to Team (2020), every transaction on the blockchain uses a lot of energy, making the average cost for each transaction between 75 and 160 US Dollars (Golosava & Romanovs, 2018). Blockchain transactions happen very slowly. Blockchain technology has just begun to gain attention, especially since 2014 (Sheldon, 2020). While blockchain technology is leading the way in many areas, its energy use is still a big problem. The energy-heavy process of mining, especially in Bitcoin and similar blockchains, has faced criticism for harming the environment (Budhi, 2020). Blockchain technology is changing industries, especially banking. It is a safe and distributed design that improves security and changes how we do international transactions, manage supply chains, handle identity, and create tokenized assets. Blockchain is still growing and developing, even though it has a lot of potential. As Kayal et al. (2020), it needs to develop in order to take the place of traditional banking methods and accept new technology.

References

[1] Abramowicz, M. (2016). Cryptocurrency-based law. *Ariz. L. Rev.*, *58*, 359.

[2] Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE transactions on dependable and secure computing*, *15*(5), 840-852.

[3] Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*(5), e109.

[4] Amiri, M. J., Agrawal, D., & El Abbadi, A. (2020, June). Sharper: Sharding permissioned blockchains over network clusters. In *Proceedings of the 2020 international conference on management of data* (pp. 76-88).

[5] Arora, P. (2020) "Top 13 Real-World applications of Blockchain Technology," *iTechnoLabs*, 28 July. Available at: https://itechnolabs.ca/top-13-real-world-applications-of-blockchain-technology/#:~:text=Blockchain%20applications%20can%20provide%20a,when%20necessary%2C%20by%20securing%20data.
[6] Atlam, H. F., & Wills, G. B. (2019). Technical aspects of blockchain and IoT. In *Advances in computers* (Vol. 115, pp. 1-39). Elsevier.
[7] Augusta, MO, Oktaviandi Syeira, CP, & Hadiapurwa, A. (2020). The Use Of Blockchain Technology In The Field Of Education. Productive: Scientific Journal of Information Technology Education,5(2), 437–442. https://doi.org/10.35568/productive.v5i2.1259
[8] Badzar, A. (2016). Blockchain for securing sustainable transport contracts and supply chain transparency-An explorative study of blockchain technology in logistics.
[9] Bagaria, V., Kannan, S., Tse, D., Fanti, G., & Viswanath, P. (2019, November). Prism: Deconstructing the blockchain to approach physical limits. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 585-602).
[10] Bandaso, T. I., Randa, F., & Mongan, F. F. A. (2020). Blockchain Technology: Bagaimana Menghadapinya?–Dalam Perspektif Akuntansi. *Accounting Profession Journal (APAJI)*, *4*(2), 97-115.
[11] Berentsen, A., & Schär, F. (2016). The fallacy of a cashless society. In *Beer C., Gnan E., and UW Birchler (Hg.), Cash on Trial, SUERF Conference Proceedings* (Vol. 1, pp. 14-19).
[12] Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K., & Hong, W. C. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*, *8*, 54371-54401.
[13] Boyen, X., Carr, C., & Haines, T. (2018, May). Graphchain: A blockchain-free scalable decentralised ledger. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts* (pp. 21-33).
[14] Budhi, V. (2020) "Advantages And Disadvantages Of Blockchain Technology," *Forbes*, 20 October. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/10/20/advantages-and-disadvantages-of-blockchain-technology/amp/
[15] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*, 1-10.
[16] Cash, B. (2017). Bitcoin cash. *Development*, *2*.
[17] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81.
[18] Chan, W. K., Chin, J. J., & Goh, V. T. (2020). Simple and scalable blockchain with privacy. *Journal of Information Security and Applications*, *58*, 102700.
[19] Chen, H., & Wang, Y. (2019). SSChain: A full sharding protocol for public blockchain without data migration overhead. *Pervasive and Mobile Computing*, *59*, 101055.
[20] Chung, M., & Kim, J. (2016). The internet information and technology research directions based on the fourth industrial revolution. *KSII Transactions on Internet and Information Systems (TIIS)*, *10*(3), 1311-1320.
[21] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE communications surveys & tutorials*, *20*(4), 3416-3452.
[22] Dai, X., Xiao, J., Yang, W., Wang, C., & Jin, H. (2019, July). Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1317-1326). IEEE.
[23] Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. *Journal of Banking and Financial Technology*, *3*, 1-17.
[24] Davis, E., et al. (2020) "Blockchain-Based Data Protection and Privacy Preservation." *Journal of Data Privacy*, vol. 4, no. 1, pp. 37-53.
[25] Decker, C., & Wattenhofer, R. (2014). Bitcoin transaction malleability and MtGox. In *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19* (pp. 313-326). Springer International Publishing.
[26] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *Financial Cryptography and Data Security: FC 2016*

International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20 (pp. 79-94). Springer Berlin Heidelberg.

[27] Ding, D., Jiang, X., Wang, J., Wang, H., Zhang, X., Sun, Y. (2019) "Txilm: Lossy block compression with salted short hashing," arXiv Prepr. arXiv1906.06500.

[28] Divya, M., & Biradar, N. B. (2018). IOTA-next generation block chain. *Int. J. Eng. Comput. Sci*, *7*(04), 23823-23826.

[29] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of network and computer applications*, *126*, 45-58.

[30] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *Ieee Access*, *7*, 45201-45218.

[31] Fernández-Caramés, T. M., Blanco-Novoa, O., Froiz-Míguez, I., & Fraga-Lamas, P. (2019). Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, *19*(10), 2394.

[32] Gartner (2017) "Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017," Gartner, Inc., Gartner Hype Cycle 2017, August 2017, Available: http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

[33] Garzik, J. (2015). Block size increase to 2MB. *Bitcoin improvement proposal*, *102*.

[34] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3-16).

[35] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512-529.

[36] Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of logic-based smart contracts for blockchain systems. In *Rule Technologies. Research, Tools, and Applications: 10th International Symposium, RuleML 2016, Stony Brook, NY, USA, July 6-9, 2016. Proceedings 10* (pp. 167-183). Springer International Publishing.

[37] Ifeng (2019) http://finance.ifeng.com/c/7rVjlivAS6v.

[38] Javarone, M. A., & Wright, C. S. (2018, June). From bitcoin to bitcoin cash: a network analysis. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (pp. 77-81).

[39] Jia, D. Y., Xin, J. C., Wang, Z. Q., Lei, H., & Wang, G. R. (2020). Se-chain: A scalable storage and efficient retrieval model for blockchain. *Journal of Computer Science and Technology*, *36*(3), 693-706.

[40] Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical foundations of computing*, *1*(2).

[41] Karm, A. (2019). Estonia – the Digital Republic Secured by Blockchain Estonia -the Digital Republic Secured by Blockchain Estonia -the Digital Republic Secured by Blockchain PwC 1. [online] Available at: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

[42] Khaerunisa, TF, & Enjat Munajat, MD (2020). A Solution To Utilize Blockchain Technology To Overcome Problems Of The Distribution Of Covid-19 Social Assistance Funds.Jane - Journal of State Administration,13(2), 264. https://doi.org/10.24198/jane.v13i2.35133

[43] Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, *20*(3), 2543-2585.

[44] Khazraee, M., Magaki, I., Gutierrez, L. V., & Taylor, M. B. (2017). Asic clouds: Specializing the datacenter. *ACM SIGARCH Computer Architecture News*, *44*(3), 178-190.

[45] Kim, J. W. (2020). Blockchain technology and its applications: Case studies. *Journal of System and Management Sciences*, *10*(1), 83-93.

[46] Kim, S., Kwon, Y., & Cho, S. (2018, October). A survey of scalability solutions on blockchain. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1204-1207). IEEE.

[47] Li, Y., & Chen, T. (2020). Blockchain empowers supply chains: Challenges, opportunities and prospects.Nankai Business Review International. https://doi.org/10.1108/NBRI-06-2020-0066
[48] Lin, C., Ma, N., Wang, X., & Chen, J. (2020). Rapido: Scaling blockchain with multi-path payment channels. *Neurocomputing*, *406*, 322-332.
[49] Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2018, July). Blockchain and IoT based food traceability for smart agriculture. In *Proceedings of the 3rd international conference on crowd science and engineering* (pp. 1-6).
[50] Lombrozo, E., Lau, J., Wuille, P. (2015) "Segregated witness (consensus layer)," Bitcoin Core Dev. Team, Tech. Rep. BIP, 141.
[51] Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99-114.
[52] Mallaki, M., Majidi, B., Peyvandi, A., & Movaghar, A. (2020). Off-chain management and state-tracking of smart programs on blockchain for secure and efficient decentralized computation. *International Journal of Computers and Applications*, *44*(9), 822-829.
[53] Marr, B. (2018). 30+ Real examples of Blockchain technology in practice. *Forbes. https://www. forbes. com/sites/bernardmarr/2018/05/14/30-real-examples-of-blockchain-technology-in-practice*.
[54] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, *8*, 100107.
[55] Nadiya, U., Mutijarsa, K., & Rizqi, C. Y. (2018, October). Block summarization and compression in bitcoin blockchain. In *2018 International Symposium on Electronics and Smart Devices (ISESD)* (pp. 1-4). IEEE.
[56] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto*.
[57] Nguyen, L. N., Nguyen, T. D., Dinh, T. N., & Thai, M. T. (2019, July). Optchain: optimal transactions placement for scalable blockchain sharding. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 525-535). IEEE.
[58] Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry?. *Journal of industrial information integration*, *17*, 100125.
[59] Poon, J., & Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. *White paper*, 1-47.
[60] Poon, J., & Dryja, T. (2016, January). *The bitcoin lightning network: Scalable off-chain instant payments*.
[61] Putri, NI, Munawar, Z., Komalasari, R., & Widhiantoro, D. (2020).Analysis of Utilization of Blockchain Technology in the Field of Education.9(2).
[62] Rahardja, U., Aini, Q., Yusup, M., & Edliyanti, A. (2020). Application of Blockchain Technology as a Media for Securing E-Commerce Transaction Processes.CESS (Journal of Computer Engineering, Systems and Science),5(1), 28. https://doi.org/10.24114/cess.v5i1.14893
[63] Reddy, B. S. (2020, January). securePrune: Secure block pruning in UTXO based blockchains using Accumulators. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)* (pp. 174-178). IEEE.
[64] Reed, J. (2017). Litecoin: An introduction to litecoin cryptocurrency and litecoin mining.
[65] Rubin, J., Naik, M., & Subramanian, N. (2014). Merkelized abstract syntax trees. *XP055624837, Dec*, *16*(3).
[66] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. *IEEE communications surveys & tutorials*, *21*(1), 858-880.
[67] Sam Daley (2020) Blockchain Voting: The Future of Elections?, Builtin. Available at: https://builtin.com/blockchain/blockchain-voting-future-elections (Accessed: 18 August 2020)
[68] Sansone, G., Santalucia, F., Viglialoro, D., & Landoni, P. (2020). Blockchain for social good and stakeholder engagement: Evidence from a case study.Corporate Social Responsibility and Environmental Management, csr. 2477. https://doi.org/10.1002/csr.2477
[69] Sarmah, S.S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), pp.23-29.
[70] Suprayitno, E., & East Cempaka, FG (2020). BLOCKCHAIN TECHNOLOGY IN THE STUDY OF ASYMMETRIC WARFARE: INDONESIAN PERSPECTIVE. Asymmetrical Warfare (PA), 8(2), 21. https://doi.org/10.33172/pa.v8i2.1435
[71] Swan, M. (2015).Blockchain: Blueprint for a new economy(First edition). O'Reilly.
[72] Utomo, TP (2020).IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN LIBRARIES: OPPORTUNITIES, CHALLENGES AND OBSTACLES.

[73] Viriyasitavat, W., Da Xu, L., Bi, Z., & Sapsomboon, A. (2020). Blockchain-based business process management (BPM) framework for service composition in industry 4.0. *Journal of Intelligent Manufacturing*, *31*(7), 1737-1748.
[74] Wang, D., Zhao, J., & Wang, Y. (2020). A survey on privacy protection of blockchain: the technology and application. *IEEE Access*, *8*, 108766-108781.
[75] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In *2016 IEEE international conference on consumer electronics (ICCE)* (pp. 467-468). IEEE.
[76] Wilda, W., & Harris, I. (2020). Penerapan Sistem Teknologi Public Blockchain Dimasa Depan Untuk Meningkatkan Kunjungan Wisata Di Kota Batam. *Jurnal Manajemen Sains Dan Organisasi*, *3*(2), 142-155.
[77] Wilson, M., et al. (2020) "Future of Data Security: A Blockchain Perspective." Future Internet, vol. 15, no. 2.
[78] Xu, Y., & Huang, Y. (2020). Segment blockchain: A size reduced storage mechanism for blockchain. *IEEE Access*, *8*, 17434-17441.
[79] Xu, Z., Han, S., & Chen, L. (2018, April). CUB, a consensus unit-based storage scheme for blockchain system. In *2018 IEEE 34th International Conference on Data Engineering (ICDE)* (pp. 173-184). IEEE.
[80] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
[81] Yang, D., Gavigan, J., & Wilcox-O'Hearn, Z. (2016). Survey of confidentiality and privacy preserving technologies for blockchains. *R3 Technical Paper*.
[82] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.
[83] Yu, B., Li, X., & Zhao, H. (2020). PoW-BC: A PoW consensus protocol based on block compression. *KSII Transactions on Internet and Information Systems (TIIS)*, *15*(4), 1389-1408.
[84] Yu, H., Nikolić, I., Hou, R., & Saxena, P. (2020, May). Ohie: Blockchain scaling made simple. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 90-105). IEEE.
[85] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.
[86] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE security and privacy workshops* (pp. 180-184). IEEE.