A Review of Security issues involved in Blockchain Technology

[1]Dr.J.Savitha, [2]Aasha.R, [3]Sangeetha.S, [4]Harshini.V.S
[1]Professor, [2]Student, [3]Student, [4]Student
B.Sc. Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore, India.

Abstract Blockchain is a one of emerging technology for decentralized and sharing of transactional data across a large peer to peer network and is widely adopted by large number of organizations due to its attractive features, where non-trusting members can interact with each other without an intermediary, in a verifiable manner. In this paper, Introduction to basics of Blockchain, Literature Review, Its Technologies, Types, Security issues involved in blockchain system, Privacy issues in blockchain technology, Applications, Conclusion

Keywords: Blockchain, Security, Bitcoin, Networks.

1.Introduction

Blockchain technology was first introduced by Satoshi Nakamoto in November, 2008. The idea was to make transactions electronically without any central authority at low transaction fee [1]. In a typical banking environment, central agencies implement concurrency control mechanism to avoid double-spending but this approach is suffering from issues like single point of failure, high transaction fee, trust issues and prone to malicious attacks [2]. In spite of the absence of central authority, the blockchain architecture is efficiently designed to maintain security, confidentiality and traceability [3][4]. In its inception, this technology was used to exchange bitcoins over the network. Bitcoin is not the only cryptocurrency based on blockchain. In fact, several cryptocurrencies are using blockchain at backend such as Ethereum, Ripple, Litecoin, Neo, Stellar and Monero. Due to its usability, now it is also being used in several other applications such as smart cities, retail, healthcare, smart transportation and authenticating IoT (Internet of Things) devices [5][6]. IoT devices are widely adopted for automation [7][8] and blockchain can prevent unauthorized access to such devices. The blockchain technology comprises of several complex concepts such as decentralized peertopeer network, the concept of mining, cryptographic puzzle, nonce, merkle root and consensus algorithms which makes it difficult to conceive for the novices. This paper is aimed at revealing the blockchain technology by explaining these complex concepts in depth along with its applications and open research challenges. Additionally, this paper is also discussing the concept of smart contracts which is the key application and future of blockchain. The rest of the paper is organized as follows: section 2 is explaining the present state of art, objectives of this paper are listed in the section 3, methodology to achieve the objectives is described in the section 4, blockchain mining process is explained in the section 5, blockchain applications and smart concepts are showcased in the section 6 followed by open research challenges in the section 7. The paper is concluded with discussion and conclusion in the section 8.

2.Literature Review

This section will present the current literature and state of the art in the area of blockchain. The articles have been found on search and indexing terms such as: blockchain, blockchain applications, blockchain survey, blockchain consensus, bitcoin, bitcoin survey, etc. The articles found in these searches have been limited to only include the most cited articles, which for example included articles with more than 70 citations as of December 2018 according to Google Scholar. We have also studied which articles that cite these articles to include chains of citations. Finally, we have divided the articles into categories based on their content and specific blockchain area. These categories are: Textbooks, Surveys Articles, and General Reports Articles that Analyze Blockchain Technology Articles on Blockchain Improvements and Variant Articles on Different Blockchain Applications Articles Discussing the Future of Blockchains However, we begin this literature review with the original bitcoin article by Satoshi Nakamoto:

2.1.Bitcoin:A peer-to-peer electronic cash system

S. Nakamoto, 2008, [6], cited by 4707 As previously stated, this article and the usage of blockchains as immutable ledgers can be seen as the origin of the blockchain technologies we see today. It is in this paper the bitcoin and blockchain revolution started. Even though the paper was published as a non peer reviewed white paper, it is one of the most cited works in the blockchain research area. The paper itself is short and does not include so many details. It primarily presents the overall idea and structure. Details on the solution, the specific technologies, and the exact properties on how the bitcoin system would be implemented is not included. Another interesting note, is that Satoshi Nakamoto never mentions the term blockchain specifically in his paper. But he does talk about chains of blocks, proof-of-work chains, and lengths of chains. A. Textbooks, Surveys Articles, and General Reports In this section we will study the different textbooks and survey articles related to blockchain. Because of their high point of view and overview perspective in writing, they tend to be good sources for the direction and understanding of a research area. One of the most well cited textbooks is by Melanie Swan, and below are the most well cited textbooks and surveys that we have found in this pre-study.

2.2.Blockchain: Blueprint for a new economy

M. Swan, 2015, [18], cited by 847 This book gives a good overview of the usage of blockchains and bitcoin as whole. As well as outlines three different versions of blockchain. Blockchain 1.0, 2.0, and 3.0. Where 1.0 can be seen as the currency, such as the original Bitcoin idea by Nakamoto. Where the blockchain is a method for a cryptocurrency, which also incorporates its own generation of the cryptocurrency as payments for the proof-of-work that has been done. Blockchain 2.0 is the next step into contracts. Meaning that it can be used for so much more than just currency in the finance world. It can for example be used in digital contracts, stocks, bonds, loans, smart contracts, smart properties, etc. Finally, the textbook explains blockchain 3.0, which extends the applications beyond the finance domain. Looking specifically into applications of government, health, science, literacy, culture and art. Where the discussions regarding government blockchains are most important for this pre-study. Including, but not limited to decentralized governance services, blockchain passports, blockchain weddings, and voting.

2.3.Mastering Bitcoin

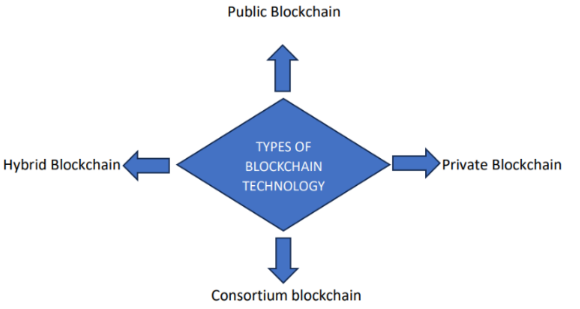
A.M. Antonopoulos, 2014 and 2017, [19][20], cited by 611 This well cited textbook exists in two editions, where both editions are well cited. The first edition had the subtitle Unlocking digital cryptocurrencies and the second edition had the subtitle Programming the open blockchain, but they have similar contents in general. the second edition mainly includes recent updates that has come to the system which was made after the first edition was published. The book itself is centered around Bitcoin, how it works, and how it is implemented using blockchain technologies. Including a deep dive into the Bitcoin reference implementation that was originally written by Satoshi Nakamoto but has been heavily modified since then. The book also explains in detail how the distributed system works and how the blockchain is managed within it.

3.Technologies

A block is a part of the blockchain in which it records all the transactions and once it is completed enters into a permanent data-base in the blockchain. In Blockchain, the blocks are linked one after other like a linked list. Every block consists the hash of the previous block Blockchain. A Linked List of Blocks Connected by Hash Pointers. Blockchain consists of a set of nodes formed like a peer to peer network. With the help of public/private keys, users can interact in the blockchain. The private key is used to sign their own transaction and is addressed in the network with the public key. It provides authentication, integrity, and nonrepudiation in the network. Each node in the blockchain makes sure that incoming transaction is valid before transmitting further. Invalid transactions are discarded. Each Blockchain network should provide certain rules for each database transaction. These rules are programmed to each blockchain client, then verifying that incoming transaction is valid or not.

4.Types of blockchain technology

There are four main types of blockchain networks: public blockchains, private blockchains, consortium blockchains and hybrid blockchains. Each one of these platforms has its benefits, drawbacks and ideal uses. Public Blockchain Hybrid Blockchain Private Blockchain Consortium blockchain.



4.1. Public blockchain

How it works. The first type of blockchain technology is public blockchain. This is where cryptocurrency like Bitcoin originated and helped to popularize distributed ledger technology (DLT). It removes the problems that come with centralization, including less security and transparency. DLT doesn't store information in any one place, instead distributing it across a peer-to-peer network. Its decentralized nature requires some method for verifying the authenticity of data. That method is a consensus algorithm whereby participants in the blockchain reach agreement on the current state of the ledger. Proof of work (PoW) and proof of stake (PoS) are two common consensus methods. Public blockchain is non-restrictive and permissionless, and anyone with internet access can sign on to a blockchain platform to become an authorized node. This user can access current and past records and conduct mining activities, the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed on the network, and anyone can verify the transactions, find bugs or propose changes because the source code is usually open source.

4.2. Private blockchain

How it works. A blockchain network that works in a restrictive environment like a closed network, or that is under the control of a single entity, is a private blockchain. While it operates like a public blockchain network in the sense that it uses peer-to-peer connections and decentralization, this type of blockchain is on a much smaller scale. Instead of just anyone being able to join and provide computing power, private blockchains typically are operated TYPES OF BLOCKCHAIN TECHNOLOGY on a small network inside a company or organization. They're also known as permissioned blockchains or enterprise blockchains.

4.3. Hybrid blockchain

How it works. Sometimes, organizations will want the best of both worlds, and they'll use hybrid blockchain, a type of blockchain technology that combines elements of both private and public blockchain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the blockchain, and what data will be opened up publicly. Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed, such as by allowing access through a smart contract. Confidential information is kept inside the network but is still verifiable. Even though a private entity may own the hybrid blockchain, it cannot alter transactions. When a user joins a hybrid blockchain, they have full access to the network. The user's identity is protected from other users, unless they engage in a transaction. Then, their identity is revealed to the other party. 4.4. Consortium blockchain How it works. The fourth type of blockchain, consortium blockchain, also known as a federated blockchain, is similar to a hybrid blockchain in that it has private and public blockchain features. But it's different in that multiple organizational members collaborate on a decentralized network. Essentially, a consortium blockchain is a private blockchain with limited access to a particular group, eliminating the risks that come with just one entity controlling the network on a private blockchain. IN a consortium blockchain, the consensus procedures are controlled by preset nodes. It has a validator node that initiates, receives and validates transactions. Member nodes can receive or initiate transactions.

5.Security issues involved in blockchain system

Blockchains mainly concentrating on three security concepts that are confidentiality, integrity, and availability. Basically, Block-chain is a distributed system, so it provides availability and all the nodes in the blockchain agreed based on a chain of transactions then the integrity of data is maintained. With the help of appropriate cryptographic keys confidentiality of transactions can be addressed. Holistic approach in Blockchain systems includes authentication and authorization of entities using the blockchain, transaction transparency, verification and communication infrastructure security, security from unauthorized insiders, compromised nodes or server failure. Blockchain systems mainly to look at security in the following aspects.

1) Ledger level security.
2) Network level security.
3) Transaction-level security.
4) Associated surround system security.
5) Smart contract security

5.1. Ledger level security

Authorized members can only participate in the blockchain. The transaction initiated by the members must be signed and valid participants create transactions in the network.

5.2. Network level security

Communication between components of different nodes must be secure from a network point of view. It must be resistant from different external and internal attack vectors in the network. The Ledger should possess the capability to withstand DoS attacks.

5.3. Transaction-level security

Transactions must be encrypted with PKI concepts so that no one compromised with unintended parties. Identity and authorization of transaction creation must be guarded i.e.only particular name.

5.4. Associated surround system security

Associated surround system components such as shadow databases should be accessed by valid users. To achieve this implement authentication and authorization mechanisms. It also involves sharing of documents to prevent from viruses, worms, and malware.

5.5. Smart contract security

Blockchain contracts or digital contracts or self-executing contracts or smart contracts acts as agreements; it can be preprogrammed with the ability to self-execute and self-enforced. Contracts loaded in the blockchain should follow the base rules given by the network. These contracts may require data from an external source that may be tampered data. To avoid this cryptographic proof must be attached; it came from the trusted source and not tampered.

6.Privacy issues in blockchain technology

One of the well-known blockchains is Bitcoin cryptocurrency. It comes with permission less blockchain ledger, so each transaction will be visible to all and anyone can verify.it seems to violate the privacy of every user. Transactional privacy and unlink ability are the two categories to provide privacy mechanism in blockchain systems.

6.1. Transactional privacy

Only the transacting parties, any regulators, and auditors should be able to see the transaction details. Participating nodes have a technique to validate the transactions considering the availability of funds, where the transaction is entirely encrypted.

6.2. Unlinkability

Arbitrary entities unable to know the details of transactions between others. It may be possible to mine the data from several transactions so that information may be useful to get the information about the parties involved in the transactions. The idea of unlinkability is about avoiding such deductions from being made.

7.Application

The blockchain was first conceivedas the mechanism supporting Bitcoin (CRYPTO:BTC). To solve the double-spending problem associated with digital currencies, Satoshi Nakamoto devised an immutable ledger of transactions that chains together blocks of data using digital cryptography. While the idea works extremely well for Bitcoin and other cryptocurrencies, there are loads of other useful applications of blockchain technology. Here are 15 of them.

7.1.Money transfers

The original concept behind the invention of blockchain technology is still a great application. Money transfers using blockchain can be less expensive and faster than using existing money transfer services. This is especially true of cross-border transactions, which are often slow and expensive. Even in the modern U.S. financial system, money transfers between accounts can take days, while a blockchain transaction takes minutes.

7.2. Financial exchanges

Many companies have popped up over the past few years offering decentralized cryptocurrency exchanges. Using blockchain for exchanges allows for faster and less expensive transactions. Moreover, a decentralized exchange doesn't require investors to deposit their assets with the centralized authority, which means they maintain greater control and security. While blockchain-based exchanges primarily deal in cryptocurrency, the concept could be applied to more traditional investments as well.

7.3. Lending

Lenders can use blockchain to execute collateralized loans through smart contracts. Smart contracts built on the blockchain allow certain events to automatically trigger things like a service payment, a margin call, full repayment of the loan, and release of collateral. As a result, loan processing is faster and less expensive, and lenders can offer better rates.

7.4. Insurance

Using smart contracts on a blockchain can provide greater transparency for customers and insurance providers. Recording all claims on a blockchain would keep customers from making duplicate claims for the same event. Furthermore, using smart contracts can speed up the process for claimants to receive payments.

7.5. Real estate

Real estate transactions require a ton of paperwork to verify financial information and ownership and then transfer deeds and titles to new owners. Using blockchain technology to record real estate transactions can provide a more secure and accessible means of verifying and transferring ownership. That can speed up transactions, reduce paperwork, and save money.

7.6. Secure personal information

Keeping data such as your Social Security number, date of birth, and other identifying information on a public ledger (e.g., a blockchain) may actually be more secure than current systems more susceptible to hacks. Blockchain technology can be used to secure access to identifying information while improving access for those who need it in industries such as travel, healthcare, finance, and education.

7.7. Voting

If personal identity information is held on a blockchain, that puts us just one step away from also being able to vote using blockchain technology. Using blockchain technology can make sure that nobody votes twice, only eligible voters are able to vote, and votes cannot be tampered with. What's more, it can increase access to voting by making it as simple as pressing a few buttons on your smartphone. At the same time, the cost of running an election would substantially decrease.

7.8. Government benefits

Another way to use digital identities stored on a blockchain is for the administration of government benefits such as welfare programs, Social Security, and Medicare. Using blockchain technology could reduce fraud and the costs of operations. Meanwhile, beneficiaries can receive funds more quickly through digital disbursement on the blockchain.

7.9. Securely share medical information

Keeping medical records on a blockchain can allow doctors and medical professionals to obtain accurate and up-to-date information on their patients. That can ensure that patients seeing multiple doctors get the best care possible. It can also speed up the system for pulling medical records, allowing for more timely treatment in some cases. And, if insurance information is held in the database, doctors can easily verify whether a patient is insured and their treatment is covered.

7.10. Artist royalties

Using blockchain technology to track music and film files distributed over the internet can make sure that artists are paid for their work. Since blockchain technology was invented to ensure the same file doesn't exist in more than one place, it can be used to help reduce piracy. What's more, using a blockchain to track playbacks on streaming services and a smart contract to distribute payments can provide greater transparency and the assurance that artists receive the money they're owed.

7.11. Non-fungible tokens

Non-fungible tokens, or NFTs, are commonly thought of as ways to own the rights to digital art. Since the blockchain prevents data from existing in two places, putting an NFT on the blockchain guarantees that only a single copy of a piece of digital art exists. That can make it like investing in physical art but without the drawbacks of storage and maintenance. NFTs can have varied applications, and ultimately they're a way to convey ownership of anything that can be represented by data. That could be the deed to a house, the broadcast rights to a video, or an event ticket. Anything remotely unique could be an NFT.

7.12. Logistics and supply chain tracking

Using blockchain technology to track items as they move through a logistics or supply chain network can provide several advantages. First of all, it provides greater ease of communication between partners since data is available on a secure public ledger. Second, it provides greater security and data integrity since the data on the blockchain can't be altered. That means logistics and supply chain partners can work together more easily with greater trust that the data they're provided is accurate and up to date.

7.13. Secure Internet of Things networks

The Internet of Things (IoT) is making our lives easier, but it's also opening the door for nefarious actors to access our data or take control of important systems. Blockchain technology can provide greater security by storing passwords and other data on a decentralized network instead of a centralized server. Additionally, it offers protection against data tampering since a blockchain is practically immutable.

7.14. Data storage

Adding blockchain technology to a data storage solution can provide greater security and integrity. Since data can be stored in a decentralized manner, it will be more difficult to hack into and wipe out all the data on the network, whereas a centralized data storage provider may only have a few points of redundancy. It also means greater access to data since access isn't necessarily reliant on the operations of a single company. In some cases, using blockchain for data storage may also be less expensive.

7.15. Gambling

The gambling industry can use blockchain to provide several benefits to players. One of the biggest benefits of operating a casino on the blockchain is the transparency it provides to potential gamblers. Since every transaction is recorded on the blockchain, bettors can see that the games are fair and the casino pays out. Furthermore, by using blockchain, there's no need to provide personal information, including a bank account, which may be a hurdle for some would-be gamblers. It also provides a workaround for regulatory restrictions since players can gamble anonymously and the decentralized network isn't susceptible to government shutdown.

8.Conclusion

Blockchains gives robust, distributed peer to peer systems and ability to interact with peers in a trustless and auditable manner. The government should provide consistent laws for this technology, and enterprise gets ready to hold blockchain technologies. Consensus mechanism is the core technology of Blockchain. In Future work, concentrate on algorithms based on consensus mechanisms of Blockchain technology for different scenarios.

REFERENCE

[1]A study on block chain technology: P S G Aruna Sri, D Lalitha Bhaskari - https://www.researchgate.net/publication/325116411_A_study_on_blockchain_technology.

[2]A survey on blockchain technology and its security: Huaqun Guo, Xingjie Yu– https://www.sciencedirect.com/science/article/pii/S2096720922000070.

[3] Block chain and its security issues and challenges:Erjon Hasanaj
https://www.researchgate.net/publication/348522832_Blockchain_and_its_security_issues_
and_challenges.

[4] A Systematic Overview of Blockchain Research: Guizhou Wang , Si Zhang , Tao Yu EMAIL logo andYuNing-
https://www.degruyter.com/document/doi/10.21078/JSSI-2021-205- 34/html?lang=en.