International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 3 ǁ 2022 ǁ PP. 20-30

A review on Blockchain-based Distributed Smart Economy Network

[1]Divya Pokkunuri, [2]Shashank Yeri, [3]Vishwa Babariya, [4]Mayank Sohani
Department of Computer Engineering)
SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering
Shirpur Campus, India

***Abstract*—** *Humans have used commodity currencies for most of their history. Fiat currency is a more recent invention, having first appeared roughly 1000 years ago and now is the most widely used kind of cash. But it's possible that this isn't the end of monetary history. Cryptocurrency is a new, experimental type of money that is neither a commodity nor fiat money. The cryptocurrency experiment may or may not succeed in the long run, but it does offer a unique combination of technical and monetary properties that present distinct economic concerns than previous forms of money.*

Security and privacy are two terms that are closely linked to current cryptocurrency trends, and this study provides an in-depth examination of both. Cryptocurrency is responsible for giving security to the flow of transactions while also regulating the creation of new currency units. The large increase in the market value of Bitcoin has led to adversaries exploiting flaws for profit. A review of the security and protection measurements of cryptocurrencies, notably Bitcoin, was conducted in this paper. This research is done for the purpose of describing cryptocurrency conventions, their utility, and communication within the framework.

Keywords*—Cryptocurrency, Cryptography, Security, Bitcoin, Blockchain, Smart Contract, Hashing algorithm, Ethereum, Mining*

Date of Submission: 05-03-2022 Date of acceptance: 21-03-2022

I. INTRODUCTION

The global economy has unmistakably moved towards the digital era in recent years. People are carrying out everything in a digital format. Cryptocurrency is the most popular trend in the digital payment industry. Cryptocurrencies, like traditional currencies, are used as a medium of exchange, but they are specifically created to exchange digital data. It's a decentralized digital currency that protects itself with cryptography, making it difficult to counterfeit. In the meantime, because it is not given by the central government, it is not taken away from the consumers. Cryptocurrency is a type of digital currency that people nowadays choose to use because it is safe and trusted. Because there is no third-party participation, cryptocurrencies give users a sense of security and reassurance when doing transactions.

Satoshi Nakamoto, a person who goes by the moniker Satoshi, wrote a research report in 2009 on a concept that would later disrupt the Internet. Since the release of the Bitcoin digital currency, over 600 different cryptographic money proposals have emerged. Bitcoin is the most successful and widely used digital currency of the many that have been developed. It has a unique data structure that may be used for storage and transactions on its network without requiring the involvement of a third party. Using decentralized methodologies, blockchain technology was created and it does not require the use of a trusted authority. The continued growth of cryptocurrencies was ensured by this amazing method. Several cryptocurrencies, such as Bitcoin, Ripple, Litecoin, and Ethereum, have also paved their way into the real world. Legitimate entities can conduct economic transactions in all of these cryptocurrencies without the need for a central authority. Bitcoin was the highest-performing operating product in 2016, and blockchain technology attained a capital market valuation of $10 billion in the same year.

These cryptocurrencies are self-contained and function without the need for a centralized regulatory authority. Bitcoin, like any other cryptocurrency, is based on peer-to-peer (or "blockchain") technology, which allows anyone who holds a unit of this money to use or spend it anywhere and at any time without the involvement of a trusted third party. Bitcoin is an open-source project that no one owns or has control over. Bitcoin, together with blockchain technology, was set up in a distributed environment and avoids the usage of single-user authority.

This research provides a thorough examination of the security and protection aspects of Bitcoin and other cryptocurrencies, as well as their underlying principles. This paper offers a description of the most recent attack vector, which includes dangers to the user's security and transaction anonymity, posing a threat to the use of cryptocurrencies in real-world applications and services. Researchers have proposed a huge variety of security solutions to address the present security and privacy concerns in Bitcoin in recent years, which are covered in this work, with particular attention on the security vulnerabilities and countermeasures that are connected to the major components of cryptocurrencies.

II. CRYPTOCURRENCY

Various regulatory authorities and academic studies have attempted to identify an appropriate definition for cryptocurrencies since the launch of bitcoin in 2008/2009 and the subsequent development of comparable cryptocurrencies [23]. Cryptocurrencies have a tough nature to define because they can represent a variety of things based on the interests of their owners and/or users.

In this capacity, a cryptocurrency can be an investment asset or a speculative asset, respectively, a new class of financial assets, a commodity, a medium of exchange or a payment mechanism, a unique fund-raising tool for businesses, as stated by Sobiecki (2015) and Feinstein & Werbach (2021)[23].

Recently, some European regulatory bodies have aligned their views on cryptocurrencies based on the EU Directive 2018/843's proposed definition. Cryptocurrencies are defined as "virtual currencies" that describe a digital representation of value and they meet the following criteria: a) The representation of the value of respective cryptocurrencies is neither issued nor guaranteed by a central bank or a public authority; b) it is not always (but maybe) associated with a legally established currency; c) cryptocurrencies do not have the legal status of money or currency; d) cryptocurrencies are accepted as a medium of exchange/payment by natural or legal persons. e) It can be electronically exchanged (mainly peer-to-peer), saved, and traded.

It is possible to categorize cryptocurrencies. One can be considered an early classification, as it relates to bitcoin's launch and market domination. The following arrangement is proposed by this classification: a) bitcoin, which stands alone and in a class of its own due to its status as the first cryptocurrency; b) altcoins, which are any other cryptocurrency that is an alternative to or different from bitcoin [23].

Another classification is commonly utilized in academic studies since it provides a better framework for examining cryptocurrencies. Based on the type of blockchains used by the individual cryptocurrency networks, this taxonomy offers the following sub-classes.

a. Cryptocurrencies based on open/public blockchains:

These cryptocurrencies are accessible via open-source software and promise a fully decentralized setting; there is no central entity that can be considered the owner and/or administrator of the respective cryptocurrency network and software; anyone can join or leave the network of the chosen cryptocurrency at any time and there is no need for a pre-approval issued by any central entity. This is the most common type of cryptocurrency, and most of the time, cryptocurrencies are intended to be used as a form of payment or exchange; they are also used for investment.

- This has a subcategory named stablecoins. Stablecoins can be backed by a fiat currency, a real object, or even a crypto-asset, or they might be based on an algorithm that attempts to ensure the value of the stablecoin remains stable [23].

b. Cryptocurrencies based on permissioned blockchains:

The networks of these cryptocurrencies grant various types of access rights to selected participants, and the networks' administrators set the rules for pre-selecting transaction validators (considered trusted participants) and the rules for their respective ledgers; in these cases, the network participants must trust the central entity that coordinates/administrates the network primarily for the purpose of selecting reliable trusted participants or nodes.

- **Cryptocurrencies based on open or public permissioned blockchains**:

These networks can be viewed and accessed by anyone; however, only authorized participants of the network can generate transactions and/or update the ledger; similarly to cryptocurrencies based on permissionless blockchains, transactions within these networks can be validated and executed without the involvement of a third (trusted) party; these cryptocurrencies, depending on the rules set by the respective networks' administrators, can be converted into tokens or flat currencies.

- **Cryptocurrencies based on closed or 'enterprise' blockchains:**

The access to these networks is limited to only those that have been approved by the administrators; additionally, only the network administrator has the ability to generate transactions and update the state of the ledger; these cryptocurrencies are frequently associated with utility tokens and are almost always considered non-convertible in fiat currencies.

	Category of Blockchain		
Properties	Public	Consortium	Private
Nature	Open and De-centralized	Controlled and Restricted	Controlled and Restricted
Participants	Anonymous and resilient	Identified and Trusted	Identified and Trusted
Consensus Pro-cedures	PoW, PoS, DPoS	PBFT	PBFT, RAFT
Read/Write Permission	Permissionless	Permissioned	Permissioned
Immutability	Infeasible to tamper	Could be tam-pered	Controlled and Could be tam-pered
Efficiency	Low	High	High
Scalability	High	Low	High
Transaction approval frequency	Long (10 min-utes or more)	Short	Short
Energy Consumption	High	Low	Low
Transparency	Low	High	High
Observation	Disruptive in terms of disin-termediation	Cost effective due to less data redundancy and higher transactions times	Cost effective due to less data redundancy and higher transactions times
Example	Bitcoin, Ethereum, Litecoin, Factom, Blockstream, Dash	Ripple, R3, Hyperledger	Multichain, Blockstack, Bankchain

Table 1. Comparison among different blockchain systems

III. ARCHITECTURE OF BLOCKCHAIN

Blockchain is a record-keeping technology that stores information in a secure, immutable, and chronological way. Defining the term, it is a chain of blocks. Blocks represent digital information and chains are said to be the public databases. It is called secure because of the advanced cryptography used to link the blocks, thus forming a chain of blocks and hence keeping the information locked inside the blockchain. It is a digital ledger that is constantly growing in a chronological manner, which means every transaction occurs after the previous one. Lastly, the term immutable has been used, which signifies that once all transactions have been built onto the blockchain, they cannot be changed [16].

Blocks are not this small to have done just one transaction. Instead, blocks depending on the size of the transaction can host thousands of transactions. In the bitcoin blockchain, one block can store 1MB of data approximately. In the "blockchain", these blocks are chained once they have recorded information.

A. PROOF OF WORK

Proof-of-Work is one of the earliest consensus algorithms. The mechanism that proof-of-work is based on is the decentralized consensus mechanism. This algorithm allows the network to come to a consensus on things like the confirmation of transactions and producing new blocks in the blockchain. With the use of proof-of-work, cryptocurrency transactions can take place without the involvement of a trusted third party in a secure manner. This mechanism also can solve the problem of double-spending where the same digital currency can be spent more than once, and it ensures that the blockchain is difficult to manipulate [2].

The way users detect if there is any form of manipulation or tampering is through hashes which are long strings of numbers that serve as proof-of-work. By putting each transaction through a hash function such as SHA-256, a hash will be generated for that transaction. If there is any form of tampering with the data that is even if only a tiny portion of the data is altered, then the result will be a hash that differs from the original hash, which indicates that there is some form of data manipulation. Before a block is added into the blockchain, there is a target value set, and any hash value below that target can only be added to the blockchain. A block that has a hash greater than the target will be rejected. The proof-of-work mechanism requires miners to go through a fierce race in order to find the nonce for a block by repeatedly putting the data through a mathematical function. This trial-and-error method for finding the valid nonce takes up a lot of computational power and hence results in the consumption of immense amounts of energy.

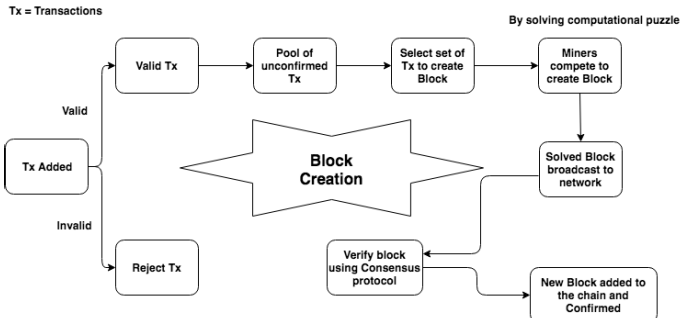

Fig 1. The block creation process in PoW procedure.

B. PROOF OF STAKE

The Proof-of-Stake mechanism was created as an alternative to the Proof-of-Work mechanism. The proof-of-work algorithm was the original consensus algorithm used in blockchains to confirm transactions and produce new blocks and add them into the blockchain. However, proof-of-work requires a huge amount of energy to fuel computational powers to run different cryptographic calculations. In proof-of-work, we have miners involved which is not the case in proof-of-stake. Instead, the participants who want to take part in validating the transactions and creating blocks must deposit a certain number of digital coins in the network as a stake. The proof-of-stake mechanism is based on deterministic algorithms, which means that in order to be the validator chosen to create the next block, it depends on the size of the stake. This simply means that the validator having the highest stake will be chosen to forge the next block. The validator in return will receive fees as a reward for each transaction. Proof-of-stake has better energy efficiency compared to proof-of-work since it does not use as much energy to mine blocks as the proof-of-work system does.

We've covered two well-known consensus methods, but there are many more. It is because of the consensus algorithms that the nature of blockchain networks is so adaptable. There isn't a single blockchain consensus algorithm that can claim to be perfect but, we suppose, that is the beauty of technology: it is always changing for the better. We'd still have to rely on Proof-of-Work if these consensus techniques didn't exist. PoW, whether you like it or not, puts the decentralization and distributed nature of blockchains in jeopardy. The following is a comparison of various consensus algorithms, along with their benefits and drawbacks.

Consensus Algorithm	Advantage	Disadvantage
PoW	Full decentralization Antiattack property	Low energy efficiency Inefficient wire transfer
PoS	Efficient wire transfer High energy efficiency	Easy to monopolize Threat to security
DPoS	High-energy efficiency	Vulnerability Less decentralization
Raft	High efficiency	Limited applications Does NOT tolerate malicious nodes
PBFT	High efficiency High safety and activity	High-communication complexity Rely on network quality

Table 2. Pros and Cons of different consensus algorithms

C. MINING

Mining involves adding transactions to the existing distributed blockchain ledger. Mining is done by creating a hash for a block of transactions that cannot be easily manipulated. The block does not contain only data, but, there are more fields in the block which impact the generation of hash. These fields are block number (a unique number for every block), data (digital documents), previous hash, and the nonce. Each block can refer to a previous block which is known as the parent block, and they can refer to the parent block through the previous hash field. Let's understand the nonce field as this new field is what mining is all about. Mining in other words is nothing but the addition of a block in the blockchain with some criteria.

The new field NONCE means Number used only once. Block number and previous hash cannot be changed. The nonce can be changed. We cannot control the hash but can vary the hash by varying the Nonce. The hash is a number (hexadecimal characters) and thus, a hash can be greater/smaller than some other hash. They are comparable once their value is calculated.

Now, for a block to enter a blockchain, what is the criteria, and what is the need for it? The criteria are that for any blockchain there is a target value set, and any hash value below that target can only be added to the blockchain. A block with a hash more than the target will be rejected. Target is an arbitrary value, and no logical

or computational explanation is required to choose the target. The reason for this type of criteria is to make the lives of miners a bit harder.
What miners do is play with the nonce in such a way that the hash value will be below the target. Their job is to vary nonce to vary the hash to make it accepted into the chain.
Once the golden nonce for which the hash will be below the target is found, the miner wins and the blockchain allows them to add their block. Once the block is added, the process continues, and further guesswork starts for the next block. The whole process of finding the hash is called a cryptographic puzzle.

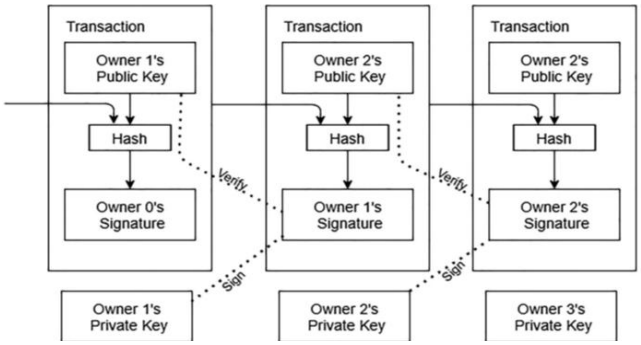

Fig 2. Structure of Blockchain

D. ETHEREUM

Ethereum is a blockchain-based open-source platform used for our application which not only tracks cryptocurrency but comes with a wide range of other functionalities. It supports hundreds of decentralized projects/applications to be built and deployed without having to build their own blockchains. Ethereum enables programmability features to developers with the help of smart contracts. Smart contracts are simply scripts that can automatically execute tasks when certain predefined conditions are met. These are self-operated contracts. Conditions are similar to 'if else' in programming [15].
The Ethereum network's coin is known as ether. Ether is used for two different purposes:

- Reimburse the mining full nodes that keep the network running. On an administrative level, this keeps things operating smoothly.
- Pay people according to smart contract terms. It is because of this that users are highly motivated to work on the Ethereum platform.
-

E. ETHEREUM PROGRAMMABILITY

The goal when developing Ethereum was to bring the same decentralization but more than just cryptocurrency [15].

- The programmability brings decentralization applications into the picture. Building and deploying decentralized applications on Ethereum blockchains.
- We can accomplish this by building a fully-fledged Turing-complete programming language into the Ethereum blockchain.
- The language offered by Ethereum is Solidity.
- Ethereum has no limitations on data types, which is not the case in bitcoins.
- Using solidity, smart contracts for our application were made.

F. WORKING OF ETHEREUM BLOCKCHAIN

- Ethereum memory stores data and code.
- When data changes, the memory state will also change which is all tracked by the Ethereum blockchain.
- When transactions occur the states change. But, in our case, it can be when a new product is added to the blockchain. Ethereum can store and maintain its states in its memory.
- Ethereum loads the program/smart contract first, executes it, and then stores the final results in the blockchain.
- This process is the same as that in our computers. The difference is that in our computers, data is stored locally while in Ethereum blockchain, the changes in state are distributed and each node has data stored in it.
- Ethereum state changes and transactions are processed by a machine EVM (Ethereum Virtual Machine).

G. SMART CONTRACT

As discussed above, Ethereum enables programmability features to developers with the help of smart contracts. Smart contracts are actually strings of computer code that can automatically execute tasks when certain predefined conditions are met. These contracts are self-operated which makes them more effective and objective [2].

All that a smart contract need is the arbitrary rules written into it.
The key when developing smart contracts is keeping the number of parties involved fixed because smart contracts can run forever.

IV. SECURITY ALGORITHMS

Blockchain is a challenging technological idea, especially given the numerous benefits that have fueled its adoption. It guarantees that information or money is exchanged in a highly secure, dispersed, and transparent manner between two parties. Many people, however, have reservations about how blockchain provides security for all parties [5].

This is where the algorithms employed for blockchain security come into play. For ensuring solid security, blockchain relies on cryptography and consensus procedures, as well as other methods. In the section that follows, an overview of the most popular blockchain security algorithms is provided.

A. SHA-256

The NSA devised the SHA-2 cryptographic hash routines, which include SHA-256. Secure Hash Algorithm (SHA) is an acronym for Secure Hash Algorithm. Cryptographic hash functions are the mathematical operations that are performed on digital data; the integrity of the data may be determined by comparing the computed "hash" (the output of the algorithm) to a known and expected hash value. Any piece of data can be used to make a one-way hash, but the hash cannot be used to generate data [5].

SHA which stands for Secure Hash Algorithm and 256 is the number of bits it takes in memory. The Hash is always 64 characters long. Each character takes 4 bits (hexadecimal hash), and so 64*4 = 256 bits space for each hash in the memory.
When compared to techniques like SCRYPT, the Secure Hash Algorithm (SHA) is far more sophisticated. Different cryptocurrencies, as well as Bitcoin itself, employ this algorithm extensively. To improve the safety of this, the processing of data blocks is practically error-free thanks to the algorithm. However, this causes transactions to slow down, and minutes are lost as a result. When SHA-256 is used, hash rates of GH/s or higher are achieved. The hash rates are required on a high level. Thereby, it is difficult for all the miners to mine and use the network.
The SHA-256 algorithm is used in quite a few aspects of the Bitcoin network:

- The proof-of-work algorithm SHA-256 is used in mining.
- To strengthen security and anonymity, SHA-256 is utilized in the establishment of bitcoin addresses.

B. SHA-3 encryption: Technology of Future

As the cost of computer processing power drops, cyberattacks become more common. By 2020, the existing digital signature will be less secure than it is now. For that reason, selecting an algorithm will be a critical decision. This is required because transient, short-term enhancements can jeopardize the security of the system. No hashing algorithm can keep a high level of security for more than ten years.
This isn't to say that cryptographers will sit about waiting for an issue to arise. The successor to Sha-2, dubbed SHA-3, has already been completed. The internet technology business will be able to employ SHA-3 as its next choice when the time comes to make that shift. However, it's possible that by then, a completely different algorithm will have been developed.

C. SCRYPT

SCRYPT, as described in the SHA-256 explanation, is a more user-friendly and speedier algorithm. In this analysis, it was discovered that newer cryptocurrencies prefer SCRYPT to SHA-256 due to more convenient and faster processes. SCRYPT uses fewer resources than SHA-256 and does not require a dedicated machine to operate, hence many miners prefer to mine SCRYPT-based cryptocurrencies over SHA-256-based cryptocurrencies. This algorithm's hash rates are in the region of KH/s or MH/s, and it can be done in a single compute operation. Because of its quick transaction turnaround time, some people are skeptical of its validity and security[5].

D. CryptoNight AND CryptoNote

CryptoNight is a proof-of-work hashing algorithm that was created by the developers of Bytecoin and CryptoNote. It was created with the intention to support CPU and GPU mining while also being resistant to Application-Specific Integrated Circuits, or ASICs. CryptoNight is a mining algorithm similar to SHA-256, which is used in Bitcoin, and Scrypt, which is used in the Litecoin protocol.

Because it can be computed by CPUs and GPUs but not by ASICs, CryptoNight was envisioned as an egalitarian hashing method. This is accomplished through the CryptoNight algorithm, which:

- Access to memory is required
- Dependence on latency

CryptoNote was first deployed in the CryptoNoteCoin protocol, which is a cryptocurrency created solely to demonstrate the CryptoNote technology. The genesis block was renewed every so often to prevent the value from accruing; CryptoNoteCoin itself has no economic worth[5].

Cryptocurrencies like Bytecoin (the first fork of the CryptoNote protocol) and Monero chose to fork from CryptoNote because of the platform's anonymity mechanism. The following are some examples of these technologies:

- Stealth Ring
- Signatures Addresses
- Adaptive Limits

A ring signature is a sort of digital signature that combines the signatures of several potential signers to create a unique signature that can authorize a transaction. A ring signature is formed by combining the real signer with non-signers to form a ring. This ring's actual signer and non-signers are both deemed equal and genuine. By ensuring that all inputs are indistinguishable from one another, ring signature technology aids the sender in masking the origin of a transaction.

By requiring the sender to produce a random one-time address for each transaction, stealth addresses provide additional protection to the recipient of a digital currency. When numerous transactions delivering funds to a stealth address are carried out, the transactions will appear on the blockchain as multiple outgoing payments to various addresses, rather than multiple payments to the same address.

Concluding, CryptoNight is a proof-of-work algorithm that was first used in the CryptoNote protocol, which has subsequently been forked by Monero and Bytecoin. The CryptoNight algorithm works by requiring memory access and emphasizing latency dependence.

V. BITCOIN

Bitcoin is the most famous and used cryptocurrency in the world. With the help of cryptocurrency, users can exchange money digitally, without the involvement of any 3rd party. Cryptocurrency works on the principle of encryption algorithms. Hashing algorithms generate unique hashes which are actually finite in number. All nodes in the network verify the transactions and the users can exchange hashes like trading physical currency. Bitcoin's singularity is maintained by the fact that there is an upper limit on its generation. The upper limit of Bitcoin is slightly less than 21 million. After that its generation will be stopped.
BitPay which is the largest bitcoin processor in the world has recently seen transaction rates grow 110% in the past 12 months (Team, 2016) [4].

The increase in transactions in Bitcoin demonstrates user acceptance. There are three aspects to Bitcoin's validity; currency, asset, and the feature which makes it possible to build other products on top of it. The increase in user acceptance instigates vendor acceptance too. It has truly proved to be a transformative technology. Bitcoin has promoted global trade and mutual prosperity.

A. Strengths:

We have discussed how its upper limit is an important aspect for its rarity and adds value. The fact that it will diminish after a certain limit is reached is important because it ensures that Bitcoin will never become inflated. This is seen as an opportunity for investors to invest as it never loses its value due to inflation. Indeed it is protected from government restrictions and changes in laws.

Bitcoin became the top-performing currency in 2015 using the US Dollar Index due to a combination of demand for a safe haven option and price volatility (Desjardins, 2016) [4].

- In 2015-2016 countries like Argentina have seen a drastic increase in usage of cryptocurrency due to the decrease in value of their currency. For Argentinians to maintain their currency value, Cryptocurrency has proved to be a legal option [4]. This was the case for many countries and investors. When the global markets

crashed, cryptocurrency usage and value has increased. In this situation, it will be safe to say that the crypto market is the only currency that can be spent and purchased with speed and efficiency and be used worldwide.

- For any other currency, to make exchanges worldwide takes time. One country's currency cannot be converted to another easily and used to perform transactions. Here acceptance plays an important role. This is not the case for Bitcoin or any other cryptocurrency. To make transactions in Bitcoin, one needs to be a part of the Bitcoin network. When you have a digital wallet with bitcoin in it, you can make transactions worldwide anytime. This is one reason one says cryptocurrency is disruptive for flat currencies.

B. Weaknesses:

Bitcoins are based on blockchain technology. Irrespective of it being known as the finest technology in terms of security, it has some internal design weaknesses. One issue is semi-anonymity. Blockchain is a public ledger, so all users can access it. Though the identity of users remains hidden, it is shared with everyone connected to the network and makes it vulnerable to some attacks.

- Bitcoins cannot handle very large transaction rates. To validate this many tests were conducted in 2016 by miners. Basically, the users using the network can only bring the network down.
- Not just Bitcoin, but digital currency, in general, can be tarnished by stories like Silk Road. Silk Road was a darknet marketplace that allowed thousands of drug traffickers and almost a million clients to conduct illegal drug transactions. Due to the lack of government tracking and semi-anonymity, Bitcoin was their preferred method of payment. It lasted from 2011 to 2013 and generated approximately one billion dollars in revenue (Bearman, 2015)[4].
- Cryptocurrencies have a reputation for being untrustworthy in terms of security. Mt Gox, which stands for Magic the Gathering Online Exchange, was the world's primary bitcoin exchange until it went bankrupt in 2011 after being defrauded of around 460 million dollars by hackers (McMillan,2014) [4]. Mark Karpeles, the CEO and key programmer did not use version control for new code. He'd also let bug and security fixes sit for weeks at a time (McMillan, 2014). Hackers were able to steal bitcoin from the exchange due to security weaknesses and oversights. When consumers sold their bitcoins for fear of it being stolen as a result of the breach, the value of Bitcoin plummeted. Ethereum, a different type of digital currency, was recently hacked for 50 million dollars (Price, 2016) [4].

The main reason for the attacks is the security standards not being up to date. It is important for the future crypto users to understand the importance of security standards and how security flaws can lead to such attacks. One solution for the same was the ‘halving event’. This causes the miners more if they use old computer hardware for the mining task. This changed the algorithm and also made it more difficult.

Fluctuations in Bitcoin can also be called a weakness. These fluctuations are directly proportional to investors' trust as it creates an uncertain trading environment. There can be investors with intentions to buy with less value and sell at a higher price, which can cause an issue.

C. Opportunities:

· Even now a great proportion of the population of developing countries are facing the issue of unbanked consumers. In 2020, globally 1.7 billion adults are unbanked, which is almost one-fourth of the total population. Cryptocurrency, being a peer-to-peer based network can help decrease these numbers. Anyone can exchange currency without the involvement of any third parties. In short, you may not have a bank account but still make currency exchanges because all one needs is access to a device such as a mobile phone in order to connect to the bitcoin network and perform the required transactions.

· Cryptocurrency offers a significant edge over traditional currencies in terms of speedy peer-to-peer transactions, particularly in international business-to-business circumstances.

· Online commerce is booming, and bitcoin is ready to expand its reach by allowing vendors and buyers to make quick and easy payments. Ebay.com a very well-known e-commerce site already employs PayPal. PayPal is a payment method that is comparable to Bitcoin and has had great success with it in facilitating all purchases made on its site.

· Individuals' general-purpose online shopping accounted for roughly 23% of Bitpay's transactions in the second quarter of 2015. (Kasiyanto, 2016). For the vendor, cryptocurrency provides a benefit over standard card-based payment methods in that it eliminates fees [4].

· At the end of 2015, the European Court of Justice declared that bitcoin transactions are not subject to value-added tax (Hileman, 2016).

D. Threats:

· The lack of centralization in blockchain causes many investors to attempt to remediate marketing problems with the help of advertisements. These advertisements can cause an issue. These organizations make the news through advertisements and can convince users to not invest. This reduces the investing company's

competition. Rules and regulations to avoid such issues are not available as the law has rarely touched digital currency.

· There is a lack of acceptance with the investors as well. There exists a list of failed startups stating security as their main reason for failure. DAO attack and other such attacks showed how inattentive investors can lose millions and simultaneously decrease their value too. Decentralization also makes securing every node in the network almost impossible.

E. ANONYMITY OF BITCOIN TRANSACTIONS

Bitcoin is based on encryption offers anonymity, but not full anonymity. We say this because it is indeed a public ledger. All the transactions that have taken place are stored in a public blockchain that is accessible by all users. There are some studies that show this anonymity can be fully removed by the transaction graphs. Removal of anonymity means the users can be identified and thus tracked to bitcoin addresses. This issue gives rise to the concept of Bitcoin mixing services. Bitcoin mixing services claim to preserve anonymity by coalescing different coins and thus, ensuring privacy [7].

For a transaction to occur, the user needs 2 inputs: Private Key and Public Key. Private keys are used for encryption and authentication and public keys are the keys that are publicly known to everyone and can individually identify a user. This is what grants the user the ownership of his/her funds. This key will be automatically generated by blockchain, and the software will sign the transaction using the same whenever a transaction is performed. This acts as an indication that the respective user has the authority to perform the transfer from the address. Similarly, the transaction also has outputs: one receiver's public key and the second being the sender of the coins. These addresses that are public are recorded in the form of a transaction graph. A transaction graph is a graph where nodes are the public keys of users of blockchain.

So, instead of directly linking/ sending bitcoins from sender to receiver, mixers are used which mix the bitcoins of multiple users and thus make it hard to find a correlation in the transaction graph [7].

F. Mixers

- When it comes to Bitcoins, the transaction is the transfer of coins from one account to another. The sender signs the transaction with his/her private key and coins are transferred to the public address mentioned in the transaction which is the address of the recipient.
- A list of previous transactions is the input for the transaction and the output is the sender and receiver's address. With the help of these, transaction graphs can be created.
- The basic idea of mixes is to mix the sender’s address with various other addresses so that it will be impossible to guess which sender has authenticated the transaction to which recipient.
- The mixer takes various inputs and encrypts them using its public key, including the destination address, a message, and a random string so that all inputs remain in the same length. The mix performs decryption to remove the extra string, encrypts it again, and sends it to all addresses of the current batch. We can also use multiple mixes to provide another layer of security. Every mix will have its own public key to encrypt the user's message. A mix will only be able to have access to the destination address and the encrypted message.
- The main goal of mixes is to maintain anonymity in blockchain by hiding the relation between sender and receiver.

G. Shared Wallets

Due to the nature of the system, all the transactions of the bitcoin are publicly stored in the blockchain. Because the origin of a transaction input must always be indicated to prevent double-spending, it is not viable to bundle encrypted transactions and transfer them anonymously. As a result, a bitcoin mixing service cannot be designed in the same way as a standard mix.

It makes no difference to the sender whether a payee receives a bitcoin that once belonged to him or a bitcoin from a random bitcoin user, providing that the total amount of bitcoins continues to be the same. As a result, mixing services can make use of the shared wallet notion. The service provider holds a set of addresses that the user can use to send bitcoins. Once payment has been validated, the bitcoins are sent to the destination address using a different address that is not linked to the first. Typically, the operator deducts a tiny transaction charge from the incoming transaction.

The main issue with all current bitcoin mixes is that they all require a central instance that preserves logs for a set period to transit bitcoins across the system. The user has no way of knowing whether or not these logs will be erased later. Furthermore, the service itself may be a potential attacker, as it would have complete knowledge of who transmits what amount of bitcoins to whom. As a result, several mixtures can be employed; however, while this reduces risk, it also increases the expense.

Three main Bitcoin mixing services are Bitcoin Fog, BitLaundry, and the Send Shared functionality of Blockchain.info. When researchers analyzed the above services using the transaction graph, it was concluded that: An attacker will find it difficult to link input and output transactions using Bitcoin Fog and Blockchain.info. They couldn't identify any direct connections in Blockchain Info's transaction graph. But while experimenting with the service BitLaundry, researchers discovered direct linkages in the transaction graph; As a result, BitLaundry cannot be considered to boost anonymity reliably [7].

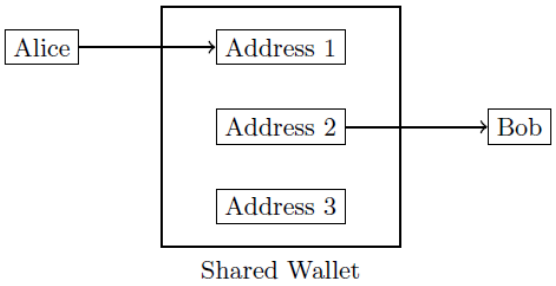

Fig 3. The shared wallet hides the relation between Alice and Bob by using a different address to pay out bitcoins to Bob.

VI. CONCLUSION

Bitcoin is one of the most well-known cryptocurrencies, having drawn not just the brightest minds who were enthralled by the concept of a decentralized blockchain, but also those who sought to exploit the blockchain's interconnectivity. There are currently 5,563 distinct cryptocurrencies in use around the world, with the number increasing every day. However, Bitcoin has always outperformed the competition in terms of usage, making it a prime target for black-hat hackers looking to commit various crimes against it. The investigation yielded findings such as how Bitcoin protocols function, including PoW and making the entire notion decentralized, requiring every user to agree on a transaction.

The attacks that potentially affect Bitcoin are outlined, as well as the countermeasures. Existing Bitcoin research projects have looked into several methods for mitigating and dealing with cyber assaults. When it comes to the absolute security of Bitcoin and the secure operation of the blockchain, however, no technique can guarantee it. Due to the decentralized nature of blockchain, issues with privacy and anonymous user characteristics have arisen. Further, we also discussed why Bitcoin is not anonymous money, how bitcoin mixes attempt to boost anonymity by utilizing the shared wallet concept, and how they differ from regular mixes in this paper.

In conclusion, the purpose of this review essay is to raise awareness of the privacy and security issues that exist in many aspects of cryptocurrencies. Following a description of Bitcoin's architecture and a discussion of how it works, this analysis focuses on the privacy and security that can be observed at various phases of the process, from transaction creation to transaction added to the blockchain. In a world where cryptocurrencies and their use are growing at an exponential rate, this paper looked into the issue of privacy as it relates to a particular user and anonymous users. In addition, the Bitcoin network's security challenges are highlighted.

REFERENCES

[1]. Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, A survey of consensus algorithms in public blockchain systems for crypto-currencies.
[2]. L. Qiao, S. Dang, B. Shihada, M.-S. Alouini, R. Nowak, Z. Lv, Can Blockchain link the future? Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2021.07.004.
[3]. Dourado, Eli & Brito, Jerry. (2014). Cryptocurrency. The New Palgrave Dictionary of Economics. 10.1057/978-1-349-95121-5_2895-1.
[4]. Peter D. DeVries (2016), An Analysis of Cryptocurrency, Bitcoin, and the Future.
[5]. T. M. Navamani (2021): A Review on Cryptocurrencies Security, Journal of Applied Security Research, DOI: 10.1080/19361610.2021.1933322
[6]. Maringmei, N & Patil, Chandrashekhar. (2021). An Analysis of Cryptocurrency, Bitcoin.
[7]. Anonymity of Bitcoin Transactions, An Analysis of Mixing Services, Malte Möser
[8]. Bitcoin Transaction Graph Analysis, Michael Fleder, Michael S. Kester, Sudeep Pillai , January 2014
[9]. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
[10]. Herrera-Joancomartí, Jordi. (2014). Research and Challenges on Bitcoin Anonymity.
[11]. B. K. Mohanta, S. S. Panda, and D. Jena, ‘‘An overview of smart contract and use cases in blockchain technology,’’ in Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2018, pp. 1–4.
[12]. Exploring the Bitcoin Network, Annika Baumann, Benjamin Fabian, and Matthias Lischke
[13]. Near Zero Bitcoin Transaction Fees Cannot Last Forever, Kerem Kaşkaloğlu, Özyeğin University, Istanbul, Turkey
[14]. Fergal Reid and Martin Harrigan. An Analysis of Anonymity in the Bitcoin System. arXiv, 2011.
[15]. A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[16]. Annu Mishra, Analytical Study on Block Chain Technology with Reference To Crypto Currency and an Overview on India's Own Crypto Currency. International Journal of Computer Engineering & Technology, 9(4), 2018, pp. 247-249.
[17]. Panda, Sandeep & Balas, Valentina & Elngar, Ahmed & Kayed, Mohamed. (2021). Bitcoin and Blockchain.
[18]. Sankar, Lakshmi & Sindhu, M. & Sethumadhavan, M.. (2017). Survey of consensus protocols on blockchain applications. 1-5. 10.1109/ICACCS.2017.8014672.
[19]. Lepore, Cristian & Ceria, Michela & Visconti, Andrea & Rao, Udai Pratap & Shah, Kaushal & Zanolini, Luca. (2020). A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics. 8. 1782. 10.3390/math8101782.
[20]. G. O. Karame and E. Androulaki, Bitcoin Blockchain Security. Norwood, MA, USA: Artech House, 2016.
[21]. Li, Wenting ; Andreina, Sébastien ; Bohli, Jens Matthias ; Karame, Ghassan. / **Securing proof-of-stake blockchain protocols**. Data Privacy Management, Cryptocurrencies and Blockchain Technology - ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Proceedings. Vol. 10436 LNCS Springer Verlag, 2017. pp. 297-315.
[22]. J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," in IEEE Access, vol. 7, pp. 36500-36515, 2019, doi: 10.1109/ACCESS.2019.2903554.
[23]. Pop, Cornelia & Colonescu, Ingrid-Emanuela. (2021). Cryptocurrencies' Puzzle. Studia Universitatis Babeş-Bolyai Negotia. 66. 99-134. 10.24193/subbnegotia.2021.2.06.
[24]. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications, Volume 126, 2019, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.10.020.