Limitations and Scope of Improvements in Blockchain Technologies

Rushil Goel
SCOPE School
VIT University, Vellore, India

Prof. Jothi K R
SCOPE School
VIT University, Vellore, India

***Abstract* — Bitcoin is one of the major applications of Blockchain technology. But with increasing use of blockchain in fields of cryptocurrency and smart contracts, the number of transactions is increasing at a much faster rate. Recent analysis proves certain limitations of bitcoin technology like scalability issues, privacy concerns, high energy consumption etc. In this paper, we analyze possibilities of blockchain improvement and examine merits and demerits of proposed solutions.**

Keywords* — *Bitcoin, Blockchain, cryptocurrency, double spending, scalability, privacy, energy consumption

I. INTRODUCTION

Blockchain is a decentralised ledger of all transaction across a peer-to-peer network. Using this technology, participating nodes can confirm and validate transactions without the need of a central authority. But with increase in use of blockchain technology in domains like cryptocurrency and smart contracts, there is an increase in number of transactions. With such an increase in usage of blockchain, the impact it has on the environment and individuals has also increased. Blockchain technology is deemed to be very secure because of its very architecture and cryptography functions and its implementations. But at the same time, it also poses some demerits such as privacy concerns, environmental impact, energy consumption, time to process a transaction, etc. One main reason why people continue to trust and use blockchain even though it has certain demerits is because of its utility and trust of people in a decentralised system. Its true that processing rate of bitcoin for a block is much lower than that of a big corporation like Visa or PayPal but at the same time its important to note that such companies are centralised while bitcoin is decentralised. Since verification of transactions is very slow in bitcoin, there is a need of innovation called Blockchain Scaling. A scaled blockchain makes the process much faster by analysing that how many confirmations are necessary to validate each transaction and limits the amount of transaction that the bitcoin network can process. Detailed theory behind this and other scopes of improvement in blockchain is what this paper focus on majorly.

II. PROBLEM DESCRIPTION

A. Problem

With increase in use of blockchain technology in domains like cryptocurrency and smart contracts, there is an increase in number of transactions. With such an increase in usage of blockchain, the impact it has on the environment and individuals has also increased. Intensive use of Blockchain has resulted in massive energy consumption, privacy concerns, concerns about high processing time per transaction etc.

A bitcoin transaction consumes about 707.6 kilowatt-hours of electricity. This is equivalent to the power consumed by an average United States household over 24 days. According to the University of Cambridge's bitcoin electricity consumption index, bitcoin miners are expected to consume roughly 130 Terawatt-hours of energy (TWh), which is roughly 0.6% of global electricity consumption.

The use of private and public keys is a crucial feature of blockchain anonymity. But it is important to note that, when a transaction is broadcasted, the details like address of sender, receiver, number of bitcoins, value of transaction, total input, total output, fees etc are visible to the entire network. This poses some privacy concerns.

The average Bitcoin block generation time is 10 minutes, which means a new block is mined every ten minutes. Based on previous assumptions, Bitcoin will average about 2,759.12 transactions per ten minutes (600 seconds). To put it another way, the Bitcoin network can only promise 4.6 transactions a second at the moment. But comparing this to processing time of big corporations like PayPal and Visa, where PayPal can process 193 transactions per second and Visa can handle 1,667 transactions per second, we realise the processing speed of bitcoin is very slow. This can be attributed to the use of high-quality computers and strong bandwidth internet connections used by big corporations.

There are ways to overcome certain demerits that the use of blockchain possess. It is important to know that wen blockchain was introduced, Satoshi Nakamoto introduced some measures to make sure blockchain is secure enough to stand among the competing companies and centralised systems.

Application of blockchain technology in world of Artificial intelligence and IoT is hindered by slow processing speed and privacy concerns. If limitations like these are addressed, then the use of blockchain in IoT can be implemented in a much more efficient manner.

III. SCALED BLOCKCHAIN

A scaled blockchain makes the process faster by analysing that how many confirmations are necessary to validate each transaction and limits the amount of transaction that the bitcoin network can process.

A scaled Blockchain makes the process of validation and transaction processing very fast without compromising security. When a transaction is added to a block and appended to the blockchain network, that transaction is mined at depth of one block. With each new block getting added to the blockchain, the depth increases by one. The transaction in a block is termed at confirmed when it reaches a depth of 6 blocks. That means when 6 blocks are successfully mined, we can say that transaction in that 7th block is confirmed and included on long term consensus.

A scaled blockchain does not sacrifice security but is expected to be fast just enough to work parallelly with internet of things (IoT) and also work with different middlemen like Visa and PayPal of the banking paradigm.

IV. THE DOUBLE SPENDING PROBLEM

Double Spending simply means using same coins more than once. Once a transaction ends on long term consensus, its impossible to spend it again. The probability of double spending is calculated by using Poisson distribution

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-\left(\frac{p}{q}\right)^{z-k}\right) \qquad (1)$$

Where,

- $\lambda = z(p/q)$
- z is the number of confirmations of transaction
- q is the attacker's percentage of Network Hash Rate
- $p = 1 - q$ is probability an honest node finds the next block

How does bitcoin handle the double spending problem?

- Let X have 1 bitcoin and he want to pay it to Y. The generated transaction (let's say T1) goes to the memory pool of unconfirmed transactions and waits to be confirmed.
- At the same time, X generates another transaction (let's say T2) stating he is paying that same coin to Z. This transaction also ends up in memory pool of unconfirmed transactions.
- Let's assume transaction T1 is taken out of memory pool first and is checked if valid. It would be stated as valid since X has 1 bitcoin and thus its added to long term consensus. Let's say now T2 is taken out, but it is termed as invalid as X does not have any more bitcoins and thus the transaction is not confirmed.
- In case both transactions T1 and T2 are being validated simultaneously, then the blockchain has 2 branches and the first transaction to reach the next block of confirmations will be confirmed.
- If T1 and T2 both successfully achieve the next block, the race for the next block will continue.
- This is the reason why it is recommended to wait for 6 confirmations for completing a transaction.

V. BLOCKCHAIN SCALIBILITY- SEGWIT

When Blockchain was introduced by Satoshi Nakamoto, he introduced a block size limit of 1 MB for each block in public blockchain. This was done as a security measure so that any block over this size limit would automatically be rejected from the peer-to-peer network. Because of this limitation, transaction processing is slowed down and blockchain is not able to keep up with processing speed of other currency payments.

Segwit (Or Segregated witness) is a solution for blockchain scalability by increasing number of transactions in a block without increasing size of the block set by Satoshi Nakamoto (As that would require intensive changes in blockchain architecture). Segregated witness helps by making space for more transactions by removing signature data from the transaction. The idea behind Segregated witness is to remove the digital signatures and store it outside the base transaction block. By doing this, we are effectively separating the "validating" part from the "effective" part thus enabling us to store more transaction into one block without changing block size. As number of transactions in a block will increase, and block confirmation is still after 6 confirmations. This means processing time per transaction decrease and number of transactions that can be processed in a second increases. The difference by separating signatures from transaction is also huge as each signature is generated using SHA256 and thus size of each signature is 32 bytes (256 bits). The digital signature takes 65% space in the transaction. If it is removed, more space is generated to store more transactions in the block.

Now the transaction is divided into 2 parts

- Non-Witness data
- Witness Data

Non-witness data (which must be stored on the block as before) and witness data (which is transferred to the expanded block) are now separated from the transaction. Each non-witness data byte is worth four weight units (WU), while each witness data byte is worth one WU. If no one uses Segwit, a block's maximum capacity is 4 kWU, which corresponds to the previous maximum block size of 1MB. The Bitcoin protocol was upgraded to Segwit in August 2017. Around 30% of transactions are conducted in a new format.

VI. BLOCKCHAIN SCALIBILITY-BLOCK SIZE INCREASE

The block size in the Bitcoin Blockchain is restricted to 1MB. There are several reasons in favour of and against increasing block size. One of the main arguments against increasing block size is that it would lead to further centralization. A node is a computer that is linked to the bitcoin network.

In bitcoin Blockchain, there are two kinds of nodes: full nodes and lightweight (or partial) nodes. Full nodes are responsible for validating every block and transaction and as a result, full nodes must keep a local copy of the entire Blockchain ledger (more than 165 GB). But on the other hand, the ledger is not stored in its entirety by the lightweight nodes. They use a simplified payment verification (SPV) mode that only involves downloading a copy of the longest proof of work chain's block headers. A miner, on the other hand, builds blocks in the Blockchain that are held by the nodes. The Bitcoin network is operated by approximately 10,000 complete nodes, with an estimated 100,000 miners. The cost of running complete nodes increases as the block size is increased. As a result, there would be less hashers operating complete nodes, and centralised organisations would gain more control, eroding bitcoin's value proposition. Increased block size benefits miners because it allows them to process more transactions per block. The amount of transaction fees a miner will earn from mining a block will increase as a result of this.

VII. BLOCKCHAIN SCALIBILITY-SHARDING

The speed at which transactions are verified is one of the most serious issues faced by cryptocurrencies.

The entire Blockchain must be stored on each complete node in the network. Sharding divides a transaction into shards, distributes them across the network, and nodes operate on individual shards in parallel. The average time taken is reduced in this manner. A standard block has a block header and a body that contains all of the block's transactions. The block header contains the Merkle root of all transactions. Sharding divides the interaction into two stages.

The transaction group is the first class, which is divided into a transaction group header and a transaction group body. Each shard is responsible for its own set of transactions. The transaction category header is split into two parts: left and right.

- The left part contains: Pre state root (state of the shard root before the transactions were applied), Post state root (state of the shard root after the transactions are applied), Shard ID and Receipt root (receipt root after all the transactions in the

shard is applied).

- The right side is crammed with validators who are selected at random to validate transactions in the shard. The transaction IDs of all transactions in the shard are stored in the transaction category body.

The second level is the standard block chain, but it has two primary roots: the state root (which represents the entire state that has been sharded) and the transaction group root (which includes all transaction groups within that block).

Sharding allows multiple concurrent transactions to occur at the same time, resulting in improved efficiency. Each transaction receipt is easily accessible from the Merkle root of the transaction community, several Merkle trees can be accessed. The receipts are also stored in a distributed shared memory that other shards can see but not modify.

Zilliqa, a new Blockchain platform focused on sharding technology that addresses the scalability problem that existing Blockchain systems like Bitcoin and Ethereum has released their public test net.

TABLE 1: COMPARISON OF CAPABILITY OF PROCESSING TRANSACTIONS IN ETHEREUM AND ZILLIQA

	Number of Full Nodes	**Number of Transactions/Sec.**
Ethereum	25,000	15-20
Zilliqa	1800	1218

And even with fewer nodes, Zilliqa can handle much more transactions per second than Ethereum or Bitcoin.

VIII. BLOCKCHAIN SCALIBILITY-PROOF OF STAKE

The proof of work protocol is used by the majority of cryptocurrencies, which means that miners mine cryptocurrencies by solving crypto-puzzles with dedicated hardware. Instead of miners, validators are present in the proof of stake protocol. As a stake, the validator must invest (lock up) some of his/her money. The validator then begins validating blocks in the following manner:

If he sees a block that he believes should be added to the blockchain, he validates it by betting on it. The validator will earn a reward equal to the stake invested if the block is added to the blockchain. The stake that the validator has invested will be taken away if he bets a malicious block. The Casper consensus Algorithm is used by Ethereum to enforce the proof of stake protocol.

The benefit of using the proof of stake protocol over the proof of work protocol is that it consumes significantly less resources and is thus more cost efficient.

TABLE 2: Comparison of Proof of Work and Proof of Stake

	Proof of Work	**Proof of Stake**
Energy Consumption	High	Low
Required Tools	Mining Equipment	No Equipment Necessary
Security	High	Untested
Decentralised Vs Centralised	Tends to Centralise	Users can remain in control of their tokens

IX. BLOCKCHAIN SCALIBILITY-DAG

Structure revolution seeks to improve the blockchain foundation's bottom structure, such as using a DAG-based or lattice-based structure. As the popularity of blockchain technology has grown, more people are joining the game. Due to the block packaging mechanism, the ever-increasing traffic causes unavoidable catastrophic congestion. As a result, the linear form of blockchain cannot escape scalability issues.

We plan to concentrate on the graph-based structure, also known as Directed Acyclic Graph (DAG), and suggest an advanced DAG-based blockchain model capable of supporting a large-scale network. Unlike conventional blockchain, which uses a linear chain topology, DAG-based blockchain does not rely on blocks to extend the network; instead, it uses a guided acyclic graph to do so. Newly produced transactions create the network in certain directions without packing into blocks by verifying the parent transactions to increase the likelihood of being verified by the next transactions. The main graph is generated with a low probability of being reversed after several iterative rounds. Greater scalability and lower transaction fees are two benefits of a DAG-based model. A linear-based blockchain, on the other hand, slows down as the number of transactions grows. The DAG, on the other hand, gets faster as the number of users grows, making it very scalable. Since there is no mining on DAGs, there is no need to charge large transaction fees to the participants. DAGs can be used in a variety of situations where blockchain isn't feasible. Nano-transactions between IoT devices and small sensors are an excellent example. IOTA's Tangle Network is a well-known project. Thus, Use of DAG also compliments use of IoT incorporated with blockchain. We will be talking about this in much more detail.

In DAG-based architectures, 3D-DAG is a scheme that consists of one mainchain and potentially one or more sidechains at a high level. In a 3D-DAG network, there are three dimensions. The basic asset-based mainchain is the first dimension of 3D-DAG, and it is based on Proof of Work consensus to provide high security and power guarantees when transferring and exchanging properties. The state-based sidechain, which provides several utilities for a smart contract, is the second dimension of 3D-DAG. It is logically based on a DAG-based framework combined with BFTstyle consensus to provide parallel processing for high efficiency. The cross-communication between the mainchain and sidechain is the third dimension of the 3D-DAG, ensuring that the inherent events flow smoothly and efficiently between DAG and chain. As a result, the functions caused by DApps can be combined.

Some rules regarding use of DAG:

Claim 1: The 3D-DAG is made up of two chains: the mainchain and the sidechain. The mainchain uses a UTXO-based chain to conduct asset exchanges, while the sidechain uses a DAG-based structure to provide a state transfer environment.

Claim 2: The mainchain uses the Proof of Useful Work (PoUW) mechanism for consensus, while the sidechain uses a modified BFT-style mechanism based on VRF.

Claim 3: To avoid DoS attacks on the DAG network, the entire DAG network is split into two layers. The first layer is the Committee, which is chosen by the miners using VRF's cryptographic sortition to validate transactions and keep the DAG sequences in order.

Expected Output by using a DAG based system is that, the key properties of 3D-DAG for qualitative outcomes are consensus achievement, including agreement, validity, and liveness. The meanings can be found in the table below. Assume that the DAG's genesis unit specifies that it needs m miners to validate transactions, and that up to b nodes of those miners are Byzantine, with m > 3b.

X. Privacy In Blockchain

Regarding the question of privacy and protection on blockchain for data management, privacy and confidentiality remains a problem for blockchain due to the fact that information is stored as a public ledger, and the methods used, such as pseudonyms, do not provide sufficient assurance. In reality, pseudonymization is not an anonymization technique, but a method for reducing the link between a data set and the original identity to which it belongs.

Any user can access and verify the details on the blockchain. Transaction tracing technology and data collection technology make it relatively simple to obtain users' identities and transaction privacy details. To address the aforementioned issues, we proposed a transaction privacy enhancement scheme based on the provable computational Diffie-Hellman problem that comes with provable security.

Because of the pseudonym used by blockchain, users in the blockchain transaction framework cannot be linked to their true identities in the real world, ensuring the privacy of the user's identity. The public existence of blockchain exposes users' addresses and transaction anonymity, but cryptocurrencies based on blockchain technology are not fully anonymous. As the number of transactions grows, attackers use data collection techniques and transaction rules to track the source of funds and extract other privacy information from accessible transaction data.

XI. SCOPE OF IMPROVEMENT - PRIVACY

A mixing transaction privacy enhancement scheme is designed to improve the ability of blockchain privacy security. To protect transaction privacy and user identity, we use a group signature algorithm and an aggregate signature algorithm, as well as a mix accountable protocol to monitor malicious users. Finally, we've created a mixing service with unlikability, anonymity, and anti-Denial of Services security.

- Anonymity: The mixing peers mix the transactions in order to obfuscate the connection between the address and the transaction user, preventing other peers from connecting addresses to users' true identities. The group signature algorithm is used to process the transaction and mixing request, so that the mixing peers only know that the transaction comes from a member of the user group, but cannot ascertain the unique identity of the user. The scheme is anonymous to both mixing and external peers, enhancing user privacy in the blockchain system.
- Anti-DoS attack: If a group of users performs a fake transaction during the mixing phase, or creates a large number of dust transactions, the final transaction will be blocked, and the final transaction will not run smoothly. The system allows for peer review and can withstand DoS attacks by malicious users. Users will be deanonymized and malicious users will be disqualified from transactions if mixed transactions are suspended or contested.
- Unlikability: Only the transaction user is aware of the link between the input and output addresses; other users are unable to map each address to the user individually.
- Application: we use mixing peers to combine multiple transactions and combine signatures into a single signature, allowing us to include more transaction records in the block. The scheme can increase signature authentication efficiency while also improving user identification and transaction privacy, and it can be easily implemented and applied in cryptocurrencies including Bitcoin.

XII. PRIVACY – MULTI SIG

Multi-signature (multi-sig) refers to the requirement of several keys rather than a single signature from a single key to authorise a Bitcoin transaction. It can be used in a variety of ways. Having multiple people share responsibility for bitcoin possession.

Similar approach can be used for sharing details of transaction as well. Multi sig setting can be generated consisting of a 2-out-of-3 signature requirement. Here, anyone who needs to check details of a transaction needs a signature from either the sender or receiver in addition to his/her signature.

- Case 1: The validator and the sender sign the requirement of checking the transaction details. Now the transaction details are visible to the validator as the sender permitted it by signing the requirement.
- Case 2: The validator and the receiver sign the requirement of checking the transaction details. Now the transaction details are visible to the validator as the receiver permitted it by signing the requirement.

- Case 3: The validator is the only one who signs the requirement. Neither the sender nor the receiver permits this action by not signing the requirement. Hence the details about the transaction are now secure and safe.
- Case 4: The sender and receiver can see the transaction details at anytime as they generated the transaction. Either way, they would be willing to sign the multi-sig requirement as the transaction was between them.

Hence in all the possible cases, using Multi-sig preserves the privacy by sharing details only with authorised users.

To synthesise several transactions into one, the scheme employs a collection of mixing peers and aggregates signature algorithms, which muddles the relationship between transaction input and output. By monitoring users' identities, malicious users are kept out of the system. While our scheme improves the privacy of users' transactions, data on blockchain remains vulnerable to leakage. In the future, we will use cryptographic strategies such as homomorphic encryption or searchable encryption to protect data privacy on blockchain.
The proposed scheme improves the system's security, reduces the system's computational overhead, and improves signature verification performance, and its effectiveness and security have been analysed and proven.

XIII. BLOCKCHAIN APPLICATONS

Blockchain technology can be used to improve IoT devices and applications. Because of bandwidth constraints, scalability issues, and costly consensus algorithms, the original blockchain structure is difficult to use in IoT. To address these issues, this paper proposes a lightweight scalable blockchain model (LSB) that provides trust and reduces the amount of time it takes to verify a transaction. The processing time to verify a transaction can be achieved in many ways. The paper covers many ways to achieve it under “Blockchain Scalability”.

By combining blockchain and IoT, data can be safely exchanged across all aspects of the supply chain. As a result, the device becomes quicker and more efficient. It may also assist companies in improving the quality of their goods and services, potentially increasing customer loyalty.

IoT security is a major concern that has hampered its widespread adoption. IoT devices are often vulnerable to security flaws, making them a prime target for Distributed Denial of Service (DDoS) attacks. DDoS attacks occur when several compromised computer systems send a large number of simultaneous data requests to a source, such as a central server, resulting in a denial of service for users of the targeted device. Several DDoS attacks have wreaked havoc on businesses and individuals in recent years. Unsecured IoT devices are a convenient target for cybercriminals who can use the devices' lack of security to launch DDoS attacks.

Another problem with today's IoT networks is scalability. Current centralised systems to authenticate, authorise, and link various nodes in a network will become a bottleneck as the number of devices linked through an IoT network increases. This would necessitate massive investments in servers capable of handling the large volume of data sharing, and the whole network could be brought down if the server went down.

In the following ways, blockchain can help mitigate the protection and scalability issues associated with IoT:

- A blockchain system's distributed ledger is tamper-proof, which eliminates the need for trust between the parties involved. The overwhelming amount of data produced by IoT devices is beyond the reach of any single organisation.
- Using blockchain to store IoT data would provide an additional layer of encryption that hackers would have to get around to gain access to the network. The blockchain technology offers a much higher degree of encryption, making it almost impossible to overwrite existing data records.
- Blockchain offers transparency by allowing anyone with permission to access the network to view and monitor previous transactions. This can be a reliable way to pinpoint the root of any data leaks and take immediate corrective steps.
- Blockchain has the potential to speed up transaction processing and improve communication among billions of connected devices. The distributed ledger technology offers a feasible solution to facilitate the processing of large numbers of transactions as the number of interconnected devices increases.
- Blockchain will help IoT companies cut costs by removing the processing overheads associated with IoT gateways by providing a way to enable trust among stakeholders.

XIV. GENERIC ESTIMATES-POW

Considering the current discussions regarding cli-mate change and sustainability, these statements could Considering the current discussions regarding cli-mate change and sustainability, these statements could Considering the current discussions regarding cli- mate change and sustainability, these statements could Considering the current discussions regarding cli- mate change and sustainability, these statements could

Considering the current discussions regarding climate change and sustainability, the widespread adoption of blockchain technology could be delayed or inhibited. Proof of Work (PoW) cryptocurrencies can, in reality, consume a disproportionate amount of energy as compared to their actual usefulness.

It's important to remember that Proof of Work blockchains' high energy consumption isn't due to unreliable algorithms or out-of-date hardware. Surprisingly, such blockchains are designed to be energy-intensive. Proof of Work blockchains are protected from attacks due to their high energy consumption: To effectively exploit or monitor the device, an intruder must have at least 25% to 50% of the total computing power that participating miners use for mining – and therefore the same proportion of total energy consumption (assuming equivalent hardware) – depending on the scenario.

As a result, the higher the value of a Proof of Work cryptocurrency, the more it is safe from attacks. Hence confirming that proof of work is indeed a thoughtful design.

To find the lower bound of the energy consumed by an arbitrary Proof of Work blockchain, we use this formula -
total power consumption ≥ total hash rate x min energy per hash

In the case of a Proof of Work blockchain, one can also calculate an upper bound for the energy required for the mining operation, assuming honest and fair miners whose sole benefit from mining is financial profit: Participation in the mining process is only profitable if the anticipated income from mining exceeds the costs associated with it:

mining rewards + transaction fees
= total mining revenue
≥ total mining costs
≥ total energy consumption
x minimum electricity price

A few easy manipulations yield the desired upper bound:

$$\text{total power consumption} \leq \frac{\text{(block reward x coin price + trans. fees)}}{\text{(avg. block time x min. electricity price)}}$$

Bitcoin's annual electricity usage was estimated to be between 60 and 125 TWh. This is comparable to Austria's (75 GWh) and Norway's (70 GWh) annual electricity usage (125 GWh). However, since cryptocurrencies currently process a small number of transactions per second, the theoretical limit is usually in the low two- or three-digit range, such as about 15 for Ethereum and Bitcoin and 100 for Bitcoin Cash. The parameters 'average block time, 'minimum size of transactions,' and 'maximum block size' are mainly responsible for this. As a result, a single transaction now necessitates enough electrical resources to meet the needs of a typical German household for several weeks or even months.

Many researchers argue that if Bitcoin could manage the volume of transactions needed by a global payment system, the resulting emissions would result in a 2°C rise in global temperature in the coming decades.

XV. Effects Of Increasing Block Size

Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could

Although Satoshi Nakamoto had fixed the block size, the blocks cannot be enlarged at will in operation. Although the block size of Bitcoin Cash has been increased by a factor of 8 (compared to Bitcoin) with no issues, a substantially larger block size is currently not possible. This is because the bigger a block is, the longer it takes the global blockchain network to spread it. This can have a negative impact on latency (the time it takes for a new block to be distributed to all nodes) and security: As a certain block propagates through the network, dividing the honest miners' money, further solutions to the puzzles are likely to be found. As a result, the network becomes more vulnerable to attack. Furthermore, since not every household can afford high bandwidth and vast amounts of hardware storage, higher requirements can lead to less decentralisation.

This trade-off has been addressed before, for example, in Bitcoin Magazine (2018). However, if global storage capacities (hard discs) and network speeds continue to develop, a significant increase in block sizes could be possible in the future. Higher transaction rates will be possible without a significant rise in energy usage.

Finally, the block reward for most Proof of Work blockchains is not constant, but is halved on a regular basis, usually every few years. Because mining fees is actually very less in comparison to block rewards, the upper bound is directly proportional to the energy price and block reward. As a result, if crypto-coin prices and power prices remain stable, it's possible that, in the long run, the energy usage of Proof of Work blockchains will halve in each of these cycles, before mining rewards are comparable to total transaction fees.

Proof-of-work has become the prevalent design of peer-to-peer cryptocurrencies since the introduction of Bitcoin. The energy use of mining has been the subject of numerous studies. The Proof of Work process necessitates a large number of computational resources, which use a lot of electricity.

XVI. PROOF OF STAKE

Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could

In Proof of stake, the importance of a participant's vote is determined by the scarce resource of capital rather than the scarce resource of computing power. The sum of cryptocurrency that the node has deposited and locked (‘‘staked") for this reason determines the likelihood of being chosen. The deposit also encourages the node to follow the network's rules, as any misbehaviour would result in the node losing the deposit.

Proof of Stake has the advantage of not requiring any computationally intensive steps, such as those needed by Proof of Work to solve cryptographic puzzles. Proof of Stake consensus has a low computational complexity and is normally unaffected by network size. As a result, it is extremely energy-efficient in large-scale systems. As a result, the energy consumption of Proof of Stake blockchains is many orders of magnitude lower than that of Proof of work blockchains, it is for this purpose that the population of Ethereum, the cryptocurrency with the second-highest market capitalization, is attempting to move from Proof of Work to Proof of Stake.

However, there are some contentious debates in the society. Some argue that eliminating Proof of work's energy consumption comes at the expense of defence, citing the fact that voting weight (capital) can only be acquired from within the system. Proof of Stake, on the other hand, has a lower propensity to centralise (due to mining's economies of scale) and is therefore more stable in the long run.

Cutting computational power and energy consumption is a good idea for the environment. It also has a financial benefit in that it should lower the rate at which new ether is issued in order to encourage validators—extra money that dilutes the value of a currency.

XVII. PROOF OF AUTHORITY

Considering the current discussions regarding climate change and sustainability, these statements could

Considering the current discussions regarding climate change and sustainability, these statements could

Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could

Blockchain technology can also be useful in constellations where only a small number of people are involved in the consensus process. Permissioned blockchains are what they're called. Many businesses, as well as the public sector, are particularly interested in them: Participants normally form a consortium, and there is a registration mechanism that ensures that all participants in agreement are identified.

As a result, there is no need to tie voting weight to a limited resource in this case, and consensus can be reached via a single-vote election.

As a result, this form of consensus process is often known as Proof-of-Identity or, more commonly, Proof-of-Authority (PoA). Proof of Authority typically refers to a range of security levels, ranging from mathematically proven and long-established completely fault-tolerant mechanisms (Paxos, PBFT) to heuristically stable algorithms like Istanbul BFT and Aura, to simple crash-tolerant mechanisms like RAFT.

Hyperledger Fabric and Quorum are two common permissioned blockchain implementations. The more stable these Proof of Authority consensus processes are, the more complicated they are and, as a result, the more energy they consume. For example, unlike Proof of Work and Proof of Stake, PBFT consensus overhead scales at least quadratically with the number of nodes in the network and is thus highly sensitive to network size. This, in essence, is related to the number of resources spent on reaching an agreement.

Low energy consumption but a small number of actors are needed for proof of authority. There is no technical rivalry between validators here, unlike the Proof-of-Work process, which is widely referred to as "mining." This consensus process requires very little computing power and, as a result, very little energy to operate.

Since the Proof of Authority only needs a small number of actors, the network may update the blockchain more regularly by shortening the time between blocks (Block time) and processing more transactions (Block size) for near-zero processing fees (Transaction fees).

There are also others in addition to these well-known consensus systems. Proof-of-elapsed-time is one example, which aims to create trustworthy random number generators using stable hardware modules. Except for some concepts that aim to create some kind of "useful Proof-of-Work," which solves puzzles that are in some way meaningful for business or research, these additional concepts usually do not include a cryptographic puzzle, like Proof of Stake and Proof of Authority. We will not analyse these consensus mechanisms in greater depth since many of these forms of consensus mechanisms are not currently used in relevant applications and have low energy requirements compared to Proof of Work.

The key takeaway from the discussion of blockchains with alternative consensus mechanisms is that, by eliminating energy intensity by design, they consume orders of magnitude less energy than Proof of Work-blockchains.

As a result, the energy usage of non-Proof of Work blockchains is unlikely to be deemed environmentally harmful. However, the form of consensus mechanism may have a major effect on energy use beyond Proof of Work and, therefore, on a completely different scale.

XVIII. THE IMPACT OF REDUNDANCY ON ENERGY CONSUMPTION

Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could

The contribution of redundant operations to overall energy consumption may be large. As a result, it's not just alternate consensus structures that need to be considered. One should consider not only ways to reduce blockchain technology's energy usage, but also principles that allow for reduced operational redundancy. Increased scalability, throughput, and privacy for blockchain solutions are the primary motivations behind all of the ideas discussed in this section that may help to reduce redundancy. Conveniently, both of these things eliminate redundancy and, as a result, reduce total energy consumption.

Reduce the degree of redundancy, i.e., the number of nodes that perform such operations, and reduce the workload associated with running a transaction are two approaches to reducing redundancy. A term known as sharding is often discussed in attempts to minimise the degree of redundancy. Sharding divides the network's nodes into subsets ("shards") and processes each transaction on only one of these subsets. The ease with which sharding can be accomplished is largely determined by the consensus process. Sharding has been discussed in this paper in the section – VII (Blockchain Scalability – Sharding).

Off-chain payment channels between two parties that communicate often are another concept for reducing redundancy. Such channels normally necessitate a blockchain transaction, during which off-chain payment channels are established and terminated. Both intermediate transactions, on the other hand, should ideally be conducted bilaterally and without involving a transaction on the corresponding blockchain. That is to say, only balances or cumulative deltas signed by members on the payment hub should be registered on-chain on a regular basis.

Reducing redundancy, on the other hand, tends to make a blockchain network more centralised, which must be carefully balanced against concerns about stability, liveness, and trust. Finding a reasonable balance between these interests could result in a reduction in the system's overall workload and, as a result, a reduction in its overall energy consumption. On the other hand, the workload associated with redundant operations, such as the inspection of new blocks, may be greatly decreased, thus mitigating the problem of redundancy.

Optimization of the computational complexity of the used cryptographic algorithms, such as those used to validate signatures, is thus a relatively simple enhancement. However, there are some natural limitations to this: Currently, all nodes operate transactions ‘‘naively," in the sense that all transaction-related data must be given on-chain, and all nodes recompute each phase independently. This could be greatly improved by just storing and verifying short correctness proofs on a blockchain and distributing the larger, plaintext data to the related participants on a separate layer. Zero-Knowledge Proofs of computational integrity, which require much less on-chain validation and communication overhead, appear to be particularly promising. Since every transaction is still checked by every node, unlike methods that reduce the degree of redundancy, these are unlikely to have a negative effect on protection.

In conclusion, there are a number of ways to reduce blockchains' inherent redundancy and, as a result, their energy consumption.

XIX. COMPARISON OF DIFFERENT ARCHITECTURES

Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could

As compared to the size of Proof of Work blockchains' energy consumption, redundancy does not add much absolute energy consumption for small networks. The natural redundancy in a blockchain, on the other hand, can lead to much higher energy consumption in large networks with many nodes. If a Proof of Stake or alternate non-Proof of Work blockchain replaces Bitcoin or another Proof of Work cryptocurrency in the future, we can expect tens of thousands of nodes to remain. Although the network's energy consumption would be low when compared to Bitcoin, it will remain high when compared to a non-blockchain centralised system with minimal redundancy.

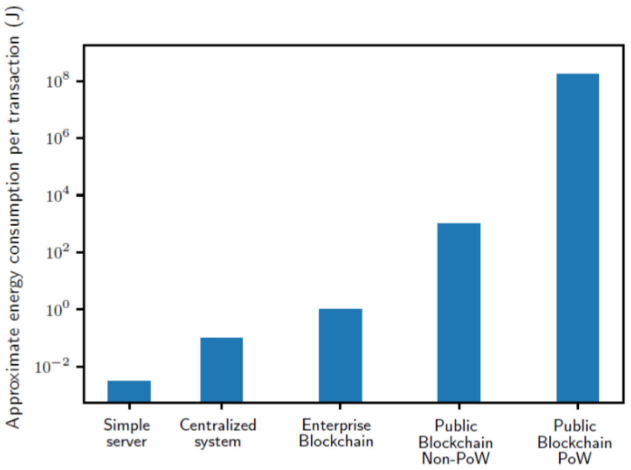

Fig. 1. comparison of the order of magnitude of energy consumption per transaction for different architectures

For various architectures, a rough comparison of the order of magnitude of energy consumption per transaction. A simple server can process transactions while using very little energy. In applications, a traditional non-blockchain, centralised system would use a more complex database and backups, increasing energy consumption slightly. A small-scale permissioned blockchain used in cross-enterprise use-cases has a similar level of redundancy, but with some additional but manageable overhead due to Proof of Authority consensus and more complex cryptographic operations, for example. Due to the high degree of redundancy, a non-Proof of Work permissionless blockchain with a large number of nodes may already consume a considerable number of resources. Energy usage is also marginal as compared to a large Proof-of-Work blockchain.

All of the figures presented here should be treated with caution because they are highly dependent on the architecture, security procedures, hardware type, and other factors. As a result, they should be treated as a rough approximation, and more precise figures have yet to be identified.

XX. BLOCKCHAIN TO SPUR ENERFY-EFFICIENT TRANSPORTATION METHODS

Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could Considering the current discussions regarding climate change and sustainability, these statements could

Some attempts to limit blockchain energy usage take a unique approach. They want to encourage energy-efficient modes of transportation, such as electric cars, using blockchain. The blockchain then encourages people to engage in environmentally friendly, conscious activities that help offset the energy used.

The shortage of infrastructure, on the other hand, is one of the key reasons why people are hesitant to invest in electric vehicles. They might live in a city with few or no electric charging stations. People who go on regular road trips may be concerned about running out of power in a remote and unknown place.

People can use blockchain-based, peer-to-peer systems to locate private charging stations for their electric vehicles. Share & Charge is one such example. It connects drivers with charging stations using the Ethereum blockchain. When they don't need to attach their electric vehicles, the owners of those power hubs will make some money on the side. All of these transactions are recorded on the blockchain and managed by the appropriate parties in a dedicated app. Projects like this could make owning an electric car more convenient and reduce range anxiety.

DRIFE, a blockchain project that brings on-demand transportation to the blockchain, is another choice. It's a decentralised framework that allows users to rate their drivers and view payment information for their trips as ledger transactions on the blockchain.

People became more familiar with the concept of using on-demand drivers to get them to their destinations thanks to companies like Uber and Lyft. DRIFE's blockchain approach aims to remove some of the issues that come with using the gig economy for transportation while also emphasising transparency. More people may decide they don't need cars if it becomes a widely available choice.

XXI. SUSTAINABLE WAYS TO MINE BITCOINS

Considering the current discussions regarding climate change and sustainability, these statements could

Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could
Considering the current discussions regarding climate change and sustainability, these statements could

As previously mentioned, cryptocurrency miners' computing setups are largely responsible for the blockchain's extremely high energy demands. Fortunately, there are attempts underway, such as Cryptosolartech's project in Spain, to mine bitcoin using solar or wind energy.

These solutions aim to reduce the associated carbon footprint and demonstrate that methods exist to enable bitcoin mining to continue indefinitely, even while using energy-intensive proof-of-work methods.

People in the business world who are considering blockchain or cryptocurrency-based systems should ask a lot of questions about how transactions are handled and how the money is mined.

The next move is to give companies or miners that use sustainable methods top priority. Northern Bitcoin, for example, is an example of what's possible. The company is one of the pioneers in the field of sustainable mining. It is driven entirely by renewable energy.

Owing to questions about its energy needs, blockchain has gained a bad reputation. Because of the aforementioned options, the blockchain which gain a better reputation among those who value its technical potential but are concerned about its energy consumption.

Outstanding blockchain ventures do not dazzle corporate decision-makers. Until pursuing blockchain solutions — and their energy consequences — the most prudent way is to thoroughly study them. They should take care to align themselves with the ones that show the most potential for true operational sustainability after collecting knowledge.

XXII. SUMMARY

The paper tries to state the limitations and problems faced by blockchain technology and tries to provide suitable improvements to overcome the same. Since 1991, the introduction of blockchain, we have seen a massive increase in use of blockchain in domains like, smart contracts, cryptocurrencies, digital identities, record keeping, legal paperwork, criminal records etc. With such a boom in number of users and increased number of transactions have resulted in mammoth merits and demerits of blockchain. Both, its advantages and disadvantages have grown multi-fold times since 1991. Today we use blockchain in both public and private sectors. The trust of people shifting from centralised systems to decentralised system is only because of their ever-increasing trust in a peer-to-peer network and public ledger. It is well known that the processing time of a transaction is very slow compared to that of big corporations like Visa and PayPal. But there are many ways to overcome this drawback that were intensively discussed in this paper. The paper clearly portrays the various demerits and proposes viable solutions that can improve blockchain's performance.

We talked about the most basic double spending problem and how blockchain tackles that. We also discussed what a scaled blockchain is and how it can be achieved. It is important to know that as much as blockchain technology is seen as secure, it is also unscalable. And this is exactly where blockchain scaling comes in. Blockchain scaling is capable of improving blockchain's performance and also suggests how moving away from Proof of Work towards another consensus algorithm can make it much more efficient. We discussed how proof of stake works and its merits. Interestingly, Ethereum is also shifting towards Proof of stake from proof of work as a result of reduced carbon footprint and also financial benefits to the company. We also figured how segregated witnesses technique helps in adjusting more transaction into a block and thus increasing the processing speed. Another way is sharding where it allows multiple concurrent transactions to occur at the same time, resulting in improved efficiency.

Structure revolution seeks to improve the blockchain foundation's bottom structure, such as using a DAG-based or lattice-based structure. DAGs can be used in a variety of situations where blockchain isn't feasible. Nano-transactions between IoT devices and small sensors are an excellent example. Use of DAG also compliments use of IoT incorporated with blockchain. The DAG gets faster as the number of users grows, making it very scalable.

We also talked about the privacy concerns that blockchain comes with. Running a decentralised ledger comes with a demerit that the details of a transaction like address of sender, receiver, number of bitcoins, value of transaction, total input, total output, fees etc are visible to the entire network. Using certain data tracking and data analysis technique, one can track the individual putting them at a risk. It its important to note that this is only possible if the activity of the individual is tracked for a while. But it is not impossible to do so either, hence the users are at a potential risk. To address this, many improvements are given, one such proposal is use of multi-Sig. We are aware how useful multi-sig is in escrow transactions. We can use the same concept even for disclosing the transaction details. The basic idea is to generate a 2-out-of-3 signature transaction that needs signature of 2 parties to reveal the details. This can help in concealing the transaction information till either the sender or the receiver approves. The proposal is an extensive use of various other algorithms and ends up protecting the privacy of the users.

Blockchain technology can be used to improve the security and scalability of IoT devices and applications. Distributed Denial of Service (DDoS) attacks are a threat to IoT devices. DDoS attacks occur when several compromised computer systems send a large number of simultaneous data requests to a source, such as a central server. By combining blockchain and IoT, data can be safely exchanged across all aspects of the supply chain. As a result, the device becomes quicker and more efficient. It may also assist companies in improving the quality of their goods and services, potentially increasing customer loyalty. This can be a reliable way to pinpoint the root of any data leaks and take immediate corrective steps. The distributed ledger technology offers a feasible solution to facilitate the processing of large numbers of transactions as the number of interconnected devices increases.

A single Bitcoin transaction consumes same amount of energy that an average United States household consumes over a month (approximately). Bitcoin has seen as much as 4,00,000 transactions per day. That's sums up to a massive amount of energy consumption. Some researchers also say that, bitcoin consumes same amount of energy as a small nation does over a year. With such a massive energy consumption, it is important to come up with methods to keep energy consumption in check. Consumed energy not only affects the environment but also increases the carbon footprint thus posing an acute risk to the sustainable development plan worldwide. Countries have started working to stop global warming and reduce use of energy in order to supplement judicious use of natural resources. This has also led to criticism towards use of blockchain on a large scale by organizations like Bitcoin and Ethereum.

Blockchain technology is designed to be energy-intensive to protect against attacks. Proof of Work (PoW) blockchains' high energy consumption isn't due to unreliable algorithms or out-of-date hardware. The higher the value of a Proof of Work cryptocurrency, the more it is safe from attacks. The proof of work is indeed a thoughtful design. Bitcoin's annual electricity usage was estimated to be between 60 and 125 TWh. This is comparable to Austria's (75 GWh) and Norway's (70GWh) annual usage. A single transaction now necessitates enough electrical resources to meet the needs of a typical German household for several weeks or even months. Many researchers argue that if Bitcoin could manage the volume of transactions needed by a global payment system, the resulting emissions would result in a 2°C rise in global temperature in the coming decades.

The bigger a block is, the longer it takes the global network to spread it. This can have a negative impact on latency (the time it takes for a new block to be distributed to all nodes) The block reward for most Proof of Work blockchains is not constant, but is halved on a regular basis, usually every few years. Higher transaction rates will be possible without a significant rise in energy usage. The upper bound is proportional to the energy price and block reward because mining fees are actually negligible in comparison to block rewards. The Proof-of-work process necessitates a large number of computational resources, which use a lot of electricity. The energy use of mining has been the subject of numerous studies. One can argue that in the long run, it's possible that the energy usage of Proof of work blockchains will halve in each of these cycles, before mining rewards are comparable to total transaction fees.

Proof of Stake consensus has a low computational complexity and is normally unaffected by network size. As a result, it is extremely energy-efficient in large-scale systems. Some argue that eliminating Proof of work's energy consumption comes at the expense of defence, citing the fact voting weight (capital) can only be acquired from within the system. Slashing computational power and energy use is not just an ecological move. It also has a financial benefit, because it should reduce the rate at which fresh ether is issued to encourage validators, which dilutes a currency's value. The sum of cryptocurrency that the node has deposited and locked ("staked") for this reason determines the likelihood of being chosen.

Blockchain technology can also be useful in constellations where only a small number of people are involved in the consensus process. The more stable these Proof of Authority consensus processes are, the more complicated they are. This consensus process requires very little computing power and, as a result, very little energy to operate. We will not analyse these consensus mechanisms in greater depth since many of these forms of consensus mechanisms are not currently used in relevant applications and have low energy requirements compared to Proof of Work or Stake. Blockchain with alternative consensus mechanisms consume orders of magnitude less energy than Proof of Work-blockchain. As a result, the energy usage of non-Proof of Work blockchain is unlikely to be deemed environmentally harmful.

Reducing the degree of redundancy, i.e., the number of nodes that perform such operations, and reduce the workload associated with running a transaction are two approaches to reducing redundancy. Sharding divides the network's nodes into subsets ("shards") and processes each transaction on only one of these subsets. Off-chain payment channels between two parties that communicate often are another concept for reducing redundancy . Finding a reasonable balance between these interests could result in a reduction in the system's overall workload and, as a result, a reduction of its overall energy consumption.

Energy usage is marginal as compared to a large Proof-of-Work blockchain. A simple server can process transactions while using very little energy. In applications, a traditional non-blockchain, centralized system would use a more complex database and backups, increasing energy consumption slightly. The figures presented here are highly dependent on the architecture, security procedures, hardware type, and other factors. They are treated as a rough approximation, and more precise figures have yet to be identified. For various architectures, a rough comparison of the order of magnitude of energy consumption per transaction is a good proxy for the total energy consumption of each transaction.

The shortage of infrastructure is one of the key reasons why people are hesitant to invest in electric vehicles. Projects like Share & Charge connect drivers with charging stations using the Bitcoin-based, peer-to-peer system. DRIFE is a project that brings on-demand transportation to the blockchain. It's a decentralized framework that allows users to rate their drivers and view payment information as ledger transactions on the ledger transactions. The project aims to remove some of the issues that come with using the gig economy for transportation while also emphasizing transparency.

It wants to encourage energy-efficient modes of transportation, such as electric cars, using the decentralized, green energy-efficiency-friendly technology. It also encourages people to engage in environmentally friendly, conscious activities that help offset the energy used.

There are attempts underway, such as Cryptosolartech's project in Spain, to mine bitcoin using solar or wind energy. These solutions aim to reduce the associated carbon footprint and demonstrate that methods exist to enable bitcoin mining to continue indefinitely. Northern Bitcoin, for example, is one of the pioneers in the field of sustainable mining. It is driven entirely by renewable energy. Owing to questions about its energy needs, blockchain has gained a bad reputation. People in the business world who are considering a cryptocurrency-based system should ask a lot of questions about how transactions are handled.

XXIII. CONCLUSION

We briefly discussed on the limitations of blockchain and how they can be mitigated. The paper proposed several improvements to increase the efficiency and performance of blockchain making its use more viable on a larger scale. Techniques like Segregated Witnesses (segwit), Sharding, increasing block size helps in making blockchain much more scalable. At the same time shifting consensus algorithm from proof of work to proof of stake also helps in making blockchain more scalable and at same time helps in decreasing the energy consumption. The privacy concerns regarding bitcoin were also addressed and suitable improvements like use of multi-sig is proposed to keep the transaction details concealed with the authorised users along with the sender and receiver. Along with this, shifting from conventional linear blockchain towards DAG or Directed Acyclic graph blockchain is also proposed and related merits were discussed briefly in the paper. Lastly, the major concern of excessive energy consumption was addressed where we delve in-depth with the statistics and proposed improvements using change of consensus algorithms, use of natural energy resources like solar and win energy to run computations etc.

REFERENCES

[1] Aleksandra Popovska-Mitrovikj, Vesna Dimitrova, Daniela Mechkaroska. Analysis of the Possibilities for Improvement of BlockChain Technology. (2018) https://www.researchgate.net/publication/330585021_Analysis_of_the_Possibilities_for_Improvement_of_BlockChain_Technology

[2] Qin Wang. Improving the scalability of blockchain through DAG. Conference Paper. (2019) https://www.researchgate.net/publication/337580877_Improving_the_scalability_of_blockchain_through_DAG

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", (2008) https://bitcoin.org/bitcoin.pdf

[4] Mechkaroska D., Dimitrova V., Popovska-Mitrovikj A: A Survey on Applications of BlockChain Technology, Proc. of the 15th International Conference on Informatics and Information Technologies CIIT, (2018)

[5] Tao Feng, Xuan Chen, Chunyan Liu, Xiaoqin Feng. Research on privacy enhancement scheme of blockchain transactions, Wiley (2019) https://www.researchgate.net/publication/335545111_Research_on_privacy_enhancement_scheme_of_blockchain_transactions

[6] R. Henry, A. Herzberg and A. Kate, "Blockchain Access Privacy: Challenges and Directions," in IEEE Security & Privacy, vol. 16, no. 4, pp. 38-45, July/August 2018, doi: 10.1109/MSP.2018.3111245. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8425613&isnumber=8425603

[7] Reid, Fergal & Harrigan, Martin. (2011). An Analysis of Anonymity in the Bitcoin System. Security and Privacy in Social Networks. 3. 10.1109/PASSAT/SocialCom.2011.79. https://www.researchgate.net/publication/51918209_An_Analysis_of_Anonymity_in_the_Bitcoin_System

[8] de Haro Olmo, Francisco & Varela Vaca, Angel & Álvarez-Bermejo, J.. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. Sensors. 20. 10.3390/s20247171. https://www.researchgate.net/publication/347021912_Blockchain_from_the_Perspective_of_Privacy_and_Anonymisation_A_Systematic_Literature_Review

[9] Koshy, Philips, Diana Koshy and P. Mcdaniel. "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic." *Financial Cryptography* (2014). https://www.freehaven.net/anonbib/cache/bitcoin-p2p-anon.pdf

[10] Sedlmeir, J., Buhl, H.U., Fridgen, G. et al. The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf Syst Eng 62, 599–608 (2020). https://link.springer.com/article/10.1007%2Fs12599-020-00656-x

[11] Dorri, Ali & Kanhere, Salil & Jurdak, Raja & Gauravaram, Praveen. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 10.1109/PERCOMW.2017.7917634. https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_and_Privacy_The_Case_Study_of_a_Smart_Home

[12] Truby, Jon. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. Energy Research & Social Science. 44. 10.1016/j.erss.2018.06.009. https://www.researchgate.net/publication/326603680_Decarbonizing_Bitcoin_Law_and_policy_choices_for_reducing_the_energy_consumption_of_Blockchain_technologies_and_digital_currencies

[13] Nair, Rajit & Gupta, Sweta & Soni, Mukesh & Shukla, Piyush & Dhiman, Gaurav. (2020). An Approach to Minimize the Energy Consumption during Blockchain Transaction. Materials today: proceedings. 10.1016/j.matpr.2020.10.361. https://www.researchgate.net/publication/344665338_An_Approach_to_Minimize_the_Energy_Consumption_during_Blockchain_Transaction