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 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

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 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

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 cli-
mate change and sustainability, these statements could

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 09, September 2022

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,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 09, September 2022

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 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

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.

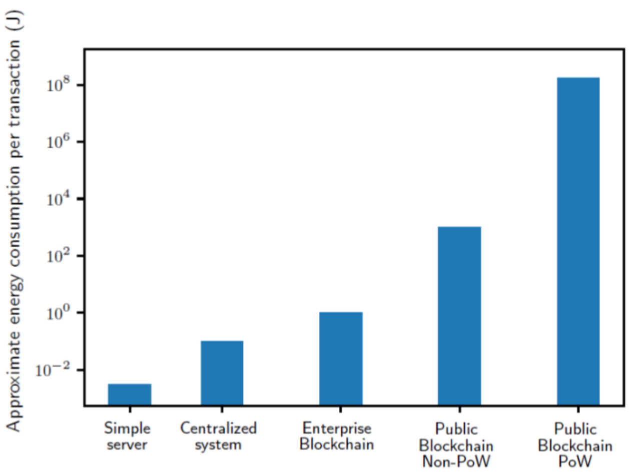

Fig. 1. comparison of the order of magnitude of energy consumption per transaction for different architectures

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 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

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

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

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

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

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

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

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

(This work is licensed under a Creative Commons Attribution 4.0 International License.)