On the way to Blockchain Sustainability Achieve Sustainability through Human Mobility : Review

M.S.W. Salgado

sahansalgado10@gmail.com

February 18, 2024

Declaration

The literature review is my original work and has not been submitted previously for any examination/evaluation at this or any other university/institute. To the best of my knowledge, it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name : M.S.W.Salgado

Registration Number : 2020/CS/154

Index Number : 20001541

Salgado 18/02/2024

Signature & Date

This is to certify that this literature review is based on the work of Mr. M.S.W.Salgado under my supervision. The literature review has been prepared according to the format stipulated and is of acceptable standard.

Supervisor Name : Prof. Kasun De Zoysa

Signature & Date

Acknowledgement

I express my gratitude to my family for their constant encouragement throughout my academic career, as well as to Professor Kasun De Zoysa and Dr. Asanka Sayakkara for their guidance and domain knowledge and Dr. Manjusri Wickramasinghe for sharing his expertise on the method of conducting a research and Academic writing through the Research Method Module.

Abstract

Since the dawn of bitcoins the blockchain technology gained an great popularity among different sectors due to its features such as decentralization, fairness immutability etc. Along with the positive impact, this also caused negative impacts for the environment, climate and the energy consumption. Algorithms like PoW was tend to consume great amount of energy, hence alternative methods such as Proof of Stake, Proof of Space have come into the play. New consensus algorithms like Proof of Review and Proof of Reputation have been introduced in recent years.

In this paper, the newly introduced human mobility based consensus algorithm known as Proof of Human mobility. This sustainable, proof based, leader selection algorithm uses the human mobility as the trust factor. The leader selection mechanism proves to be fair, since the probability relies on the ability to being active. In the latter part this algorithm will thoroughly analyzed.

Keywords : Human Mobility, Blockchain, Sustainability, Consensus

Contents

List of Figures

List of Tables

AI	Artificial Intelligence
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Activity
DPoS	Delegated Proof of Stake
PoHM	Proof of Human Mobility
MCS	Mobile Crowd Sensing
TPS	Transactions per second
DoS	Denial of Service
NFC	Near Field Communication
IB	Initialization Block
TTP	Trusted Third Party
SPV	Simplified Payment Verification

1 Introduction

In recent years the blockchain has become the transforming force behind different industries (Wüst & Gervais 2017). The introduction of Bitcoin (Warmke 2024)has gained a great popularity among the society, with the promise of decentralization, security and transactions without third parties. But recent years, the traditional consensus algorithms (Proof of Work, Proof of Stake) started to face criticisms due to the energy consumption, centralization and not being sustainable.

Therefore researchers have been exploring new and sustainable consensus algorithms, which can not only address sustainability but also empower primary strengths of blockchains. One such approach proposed by Kongahage et al. (2022) is the usage of human mobility as a trust factor for block creation. Since the natural human behaviour is used within this algorithm, it might provide health benefits and also rewards for being active. Since the Smart Mobility and Mobile Crowd Sensing (MCS) technologies have been developed and enhanced over the past years, these technologies might be useful track human mobility patterns. Since the blockchain technology gets adopted in different industries, Karger et al. (2021) and Huang et al. (2020) researched on how to adopting blockchain affects smart mobility and MCS. The research of Kongahage et al. (2022) have discussed a mechanism to involve human mobility and have introduced a novel blockchain algorithm.

The review follows the following structure. Section 2 discusses the background details of blockchains and sustainability. Section 3 discusses some existing consensus algorithms. Section 4 and 5 will discuss the proposed algorithm of Kongahage et al. (2022) and the evaluated results of the research. Section 6 will critically analyzes the Proof of Human Mobility (PoHM) algorithm followed by Section 7 which discusses the future works to be done.

2 Background

2.1 Structure of a Blockchain

The blockchain is a ledger, which consists of several blocks in a sequence. Each node in the network keeps and maintains the same local ledger in a distributed manner (Zhang et al. 2021). A simple blockchain is depicted in the figure 1. A block consists of block header and a block body. The parts of a block header are (Zheng et al. 2018),

- Version – Set of block validation rules
- Previous block hash
- Merkle hash
- Timestamp
- nBits – compacted current hashing target
- Nonce – 4 byte field, increases for every hash calculation starting from 0

And the body of the block consists of transactions and transactions counter. Each user has its own private key (K^{prv}) and a public key (K^{pub}), usually stored in a personal wallet(Zhang et al. 2021). In the signing phase the private key is used and in the verification phase, the public key of the signed private key's owner will be used. This is known as the digital signature. In untrustworthy environments a digital signature is used to validate the transactions.

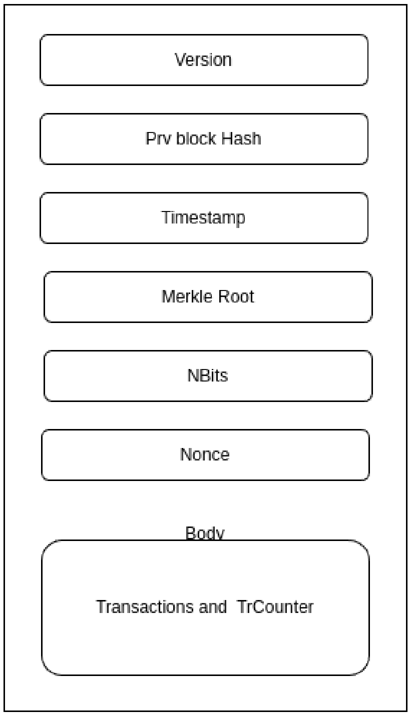

Figure 1: Block Structure

2.2 Taxonomy of Blockchains

Key features of Private, Public and Consortium Blockchains are diplayed in following table (Ghosh et al. 2020).

Parameters	Private	Consortium	Public
Central Authority	Full	Partial	Decentralized
Read Access	Decided by Org	Decided by Org	Public
Speed	Fast	Slow	Slow
Identities	Known	Pseudonymous	Anonymous
Authentication	Required	Required	Not Required

Table 1: Taxonomy of Blockchain.

2.3 Characteristics of Blockchains

Decentralization : Rather than the using the traditional validation of transactions with central authority, blockchain uses P2P transactions without the interference of central authority, hence mitigating performance downgrades. Therefore nodes can operate according to established rules(Zheng et al. 2018).

Persistence/Immutability : Each transaction spread across network and validated by other nodes, therefore it is not easy to tamper and easy to detect frauds. Since every node has own local backup, it is very costly to tamper with each and evry local copy of the ledger(Zheng et al. 2018).

Anonymity : No central being to store user nodes' private information. And user nodes also have the ability to interact in the network with generated address or further they can generate more addresses to protect identity(Zheng et al. 2018).

Auditability/ Traceability : Users can trace and verify previous records since each transaction in the blockchain consists of verification and also a timestamp. The private information of the nodes are encrypted with asymmetric cryptography. This makes the whole blockchain traceable and transparent(Zheng et al. 2018).

Autonomy : The blockchain system's members have established automatically specified protocols and specifications based on rules and algorithms, which each node must adhere to in order to guarantee authenticity and accuracy.(Zhang et al. 2021).

2.4 Why decentralization is important

Blockchain was primarily implemented with decentralization in mind. The core idea of the word 'decentralization' means power distribution across blockchain and being fair to everyone on the network.Within some consensus algorithms (eg : Proof of Work), individuals gather together for the mining process. This also causes problems in the security factor, and these security discussion will be done in subsection 2.9. These so called 'mining pool' may have more computational power than other user nodes in the network. This may cause the power of the network to be biased towards these individuals and to make the network more centralised than decentralized. Proof of Stake (PoS) is more sustainable consensus algorithm than the Proof of Work (PoW) consensus algorithm, and this is based on leader selection which also causes decentralization in the network. More of the consensus algorithms will be discussed in section 3 (Kwon et al. 2019).

Even though the decentralization concept is much important to a blockchain,Kwon et al. (2019) has depicted that it is difficult to design a system with full decentralization by proving contradiction between full decentralization and the reliance of Trusted Third Party (TTP).

2.5 Consensus Process Model

Fu et al. (2021) has found out both DAG and chain structured blockchains have internal connections, after the analysing of consensus algorithms. Based on this Fu et al. (2021) proposed a unified process model for the consensus algorithm with three phases namely, accountant selection, block addition and transaction confirmation.

Accountant selections: Accountants are responsible for block generation, integration of transaction into blocks and block sending. Here inputs are transaction and all nodes and outputs are accountant and new block.

Block Addition: A node erifies both accountant and the block. If valid then new block will be added to the blockchain.

Transaction Confirmation: After above two phases the local ledger has the new blockchain. With the votes from the nodes, the new block is added to the chain. If there are any inconsistencies with nodes, then even if the block is added it is not confirmed.

2.6 Consensus Types

Leader based: This algorithm primarily focuses on accountant selection and PoW and PoS can be identified as some examples. In PoW nodes use their computational power to solve a puzzle and the winner adds new block. In PoS uses the stakes each and every node has and use them to decide the winner, which is much more sustainable but higher probability of being biased. Additional enhancements (such as Delegated Proof of Stake (DPoS)) and some other algorithms like Proof of Luck, and Proof of Burn make efforts to balance security and other blockchain properties.

Voting : In this mode a structured process which involves all users used to make group decisions. This ensures agreement among the user nodes of the network. Different voting mechanisms (Byzantine Fault Tolerant (BFT), Delegated Voting) can be used to achieve this.

In addition to those consensus types Fu et al. (2021) has offered some insights on Committee+ voting ode and Fair Accounting mode.

2.7 Sustainability

Sustainability in blockchains has become a great concern in society within recent years. Since these technologies are getting adopted in many different scenarios, the environmental and human health impacts of blockchain should be considered.

One of the primary main reasons to improve sustainability is the huge energy consumption of blockchains for their relevant operations such as crypto mining. As mentioned before the PoW algorithm used in Bitcoin, demands intense amount of computational resources for Mathematical guessing process which is really useless for real life situations. Gallersdörfer et al. (2020) and Goodkind et al. (2020) have researched and found out that, since mining alone consumes great amount of energy, many concerns on its carbon footprint and contribution to climate changes have arisen.

The need of high computational power not only threatens sustainability but also cause barriers among the user nodes in the blockchain networks. Therefore some kind of technological innovation, rules and regulations or alternative consensus algorithms like PoS, Proof of Activity (PoA) should be introduced (De Vries 2023).

Research of Gundaboina et al. (2022) has conducted the possibility of using renewable energy to mining process. Also It depicted how overclocking of GPU affect the performance of mining though it increase the energy consumption. It has mentioned how the use of sustainable energy provides more profit for the miners while creating a significant positive impact on the environment.

The study of Jayawardhana & Colombage (2020) have provided a conceptual overview of how to address issues related to sustainability through responsibility and governance and the potential of Blockchain to address sustainability.

The research of Kongahage et al. (2022) has introduced a new blockchain consensus algorithm known as Proof of Human Mobility, which is a way more sustainable than current algorithms in use and improves human well being. More of the details of this algorithm ill be discussed in section 3.

2.8 AI and Blockchain

Artificial Intelligence (AI) and blockchain are the two most popular technologies in the present. The research of Zhang et al. (2021) has discussed how AI empowers blockchain and also how blockchain empowers AI.

The transparency and the traceability of data sources is important to securely share data. Transparency can be achieved by the synchronisation of ledger in the blockchain and the traceability can be assured by the timestamps and the digital signatures.

If any party from available parties misbehaves then it should results an economic penalty while honest nodes receive incentives. These can be automated and if needed these can be validated using smart blockchain technologies which improves fairness.

Predefined rules and auto execution characteristics of smart contracts can be used to mitigate the possibilities of attack and unpredictability.

New Cryptography technologies can be used to withstand malicious attack and also direct or indirect private information leaks hence improves privacy.

Rather than the use of central server to handle all the AI tasks, the computing capacitity can be distributed, therefore can be used to handle new and large while increasing performance.

The thousands of parameters included in blockchain can be handled and simplified by AI to make better decisions, optimize and reduce human errors.

Smart Contracts can be improved and the blockchain can be empowered with intelligence with the integration of AI.

The industrial sector adopts the blockchain technology nowadays, but face database limitations which causes low query execution rate. AI can empower to efficiently manage storage or increase efficiency through continuous learning.

Even though AI is very useful tool to use with blockchain technology, Zhang et al. (2021) has also pointed out some research issues with the very topic in Sharing Applications, Security Applications, Transaction Applications, Deposit Applications, Resource Management Applications and Scalability optimization Applications. And Privacy, Scalability, Security have been found out as the challenges.

2.9 Blockchain Challenges

Blockchain technology has now gained a lot of attention due to its ability to revolutionize and modernize various sectors including industrial and financial sectors. Therefore the concern about the security of blockchain should also be concerned, since it provides some of the most powerful protection for data tampering, unique security challenges have arisen which need to be mitigated. The Reviews of Lin & Liao (2017) and Fu et al. (2021) have offered great insight about issues and challenges of blockchain technology.

Badawi & Jourdan (2020) has discussed 66 attacks on cryptocurrencies and have analyzed and have proposed a possible defensive mechanisms.

Double spending is an attack for blockchain where the malicious node creates a fork to revoke a transaction before its confirmation. Since these are targeting transactions which are not confirmed immediately after addition, the possibilities of revoking a non-confirmed transaction should be mitigated.

Denial of Service (DoS) attacks plans to make the resources unavailable for the users of the network by disrupting the host of the network. These can be mitigated by lowering the single-point failures, specifically the accountant node. Therefore selection of accountant node should be unpredictable and also should develop mechanisms to handle failures if occurred.

The **Sybil attack** could cause centralization and unfairness among nodes by creating multiple identities to gain control over the blockchain network. In this kind of situation authentication of identity also matters.

Majority Attack / 51% attacks occur in algorithms like PoW, where the Blockchain relies on miners' computational power. Miners can gather and create mining pools, and if the total power of that pool becomes 51% or more of the network's total power, the network becomes biased toward the pool, which causes centralization and security risks.

As the blockchain grows with more and more data, storing and computing those data becomes much more harder and the time it gets to synchronize data among all nodes will be higher. The review of Lin & Liao (2017) has mentioned Simplified Payment Verification (SPV) technology which only uses blockchain header messages. Lin & Liao (2017) has also mentioned about some challenges such as Time confirmation, Regulation Issues and Integrated Cost issues of Blockchain.

The **Fork problems** occur due to the disagreement among nodes due to the changing of consensus rules. This creates possibilities for Hard or Soft forks. When the blockchain system upgrades to a new version, where old version is not compatible with the old version, the chain will be splitted to different chains. Unlike Hard forks, the nodes in the blockchain with soft fork, continue to work together despite the differences. The old nodes gradually becomes updated but since old nodes are unaware about the rule changes, this scenario goes against the the principle of all nodes being able to verify (Lin & Liao 2017).

3 Consensus Algorithms

In this section, the most notable consensus algorithms in use and a few recent researches of new algorithms will be discussed.

PoW: This is used to make an agreement on transactions by involving user nodes known as miners to compete in solving a complex mathematical puzzle. This algorithm allows anyone to participate in the mining process, hence provide decentralization. But recently this plays a crucial role in the sustainability, due to its massive energy consumption rates (Wagner et al. 2019).

PoS/DPoS: Unlike PoW, validators of the transaction use the amount of cryptocurrency they hold as a stake, ensuring they are more likely to be selected as the leader to create new blocks. Compared to PoW this more energy efficient, but causes some issues related to blockchains such as the possibility of becoming centralized. DPoS aims to improve the efficiency by reducing the number of participants during the validation and block creation process (Wagner et al. 2019).

PoA: This algorithm consists of two phase operation. Initially it uses PoW to create the initial block and uses PoS to validate the transaction. This ensures energy efficiency and decentralization (Bentov et al. 2014).

Proof of Space: This algorithm allows user nodes to prove that they have certain amount of disk space, which is much more efficient and sustainable than intense mathematical computations. (Dziembowski et al. 2015).

Also recent researches have introduced new consensus algorithms, such as Proof of Review and Proof of Reputation.

Proof of Review: This algorithm forces the participant nodes to act honestly, and to maintain a positive behaviour. Also the nodes are allowed to provide review other nodes and rate them in the form of stars, which allows nodes to gain trust with good ratings and wise versa. Also Khan et al. (2021) has already mentioned that this algorithm may be vulnerable to attacks such as Sybil attacks.

Proof of Reputation: This is similar to the Proof of Review . The nodes are weighted with the reputation it has. The ratings are offered through previous interactions between user nodes (Aluko & Kolonin 2021).

4 Proof of Human Mobility Discussion

Kongahage et al. (2022) has proposed a much more sustainable blockchain algorithm which involves human mobility as a trust factor. This is not only sustainable but also healthy for the participants in the network. This section is reserved for the explanation of the proposed solution.

4.1 Architecture of the Algorithm

Two keys, namely public key K_{pub} and private key K_{prv} pair inside the PoHM network identify a specific device as a mining node, which is a mobile device equipped with a short-range communication technology, which enables connection with other nodes nearby. Nodes are further connected to a suitable peer-to-peer network protocol. Creating a blockchain instance and transferring the complete blockchain ledger to local storage is all that is required for a miner node to join the network.
PoHM will choose a location mfor the user to go to start the consensus process. When two users arrive at the spot, PoHM will detect human motion by the short-range communication device to confirm the users' whereabouts.

A node can play two roles in short-range communication, which are prover and verifier. A ticket is a confirmed user's location. These tickets are used to choose the blockchain's next leader(Kongahage et al. 2022).

4.2 Capturing User Mobility

A mobile human being is one that moves from one place to another. Thus, capturing human movement means confirming that a person arrived at some location from a another location within a given amount of time.

Kongahage et al. (2022) proposes a community-based verification system which is fair and competitive, with nodes using each other to confirm their existence at the place in according to a predetermined protocol. A node's likelihood of being chosen as the leader mostly depends on its capacity for human mobility.

A location is any easily accessible area close to a node, usually a public area. Every node will have a list of locations, and a single location can be shared by several user nodes. A ticket can be identified as an opportunity to be chosen as a leader. A node has to demonstrate their identity to the network and participate in constant mobility in order to create a ticket. Mobility, or moving between sites, is an continuous activity where a user can run or walk. A node's likelihood of being chosen as the leader increases with the number of locations it visits and the tickets it generates.

4.3 Human Mobility

Kongahage et al. (2022) has introduced any easily accessible place near a node, usually a public place, is referred to as a location. Each node will have a list of locations, and several user nodes may share a same location. A ticket is a chance to be selected as a leader. To produce a ticket, a node (a miner or user) must identify themselves to the network and engage in continuous mobility. The more places a node walks or runs and tickets it creates, the more likely it is to be selected as the leader.

4.4 Initialization Block

The relevant miner who gets selected as the leader should create the Initialization bock for location generation.A single ticket is generated by an Initialization Block (IB), which is made up of a certain number of tickets. To make a single ticket, a collection of tickets is consumed in this instance. But the ticket pool will run out if this loop keeps on, which will put the entire system in a deadlock. To prevent that kind of a scenario, same ticket is picked several times into the IB with an upper bound in order to prevent this scenario. The upper bound prevents the same set of tickets from being chosen every time. The tickets list in IB is hashed using Merkle hashing (Kongahage et al. 2022).

4.5 Location Generation

After generating a location The node should arrive at the generated location, where a new ticket is created when the node's presence is confirmed.

The tickets hash (Merkle hash of the tickets) of the IB is hashed in order to get a pseudo-random number N, which is then used to choose a location. Since the value N is arbitrary and unpredictable as a randomly chosen fixed number of tickets will always result in a random and unpredictable hash. Here, the hash function/random number generator uses the tickets hash HashM erkle (tickets) as its seed.

$$N = Hash(Hash_{\text{Merkle}}(tickets)) \tag{1}$$

Before the user gets to the place, the N is unknown to the other nodes to ensure that a node's location remains private from other users hence important to privacy and security.

However, the verifier will confirm that N is randomly generated using the tickets in IB during short-range location verification.

To select a place from the location list, one can utilize equation 2's random value, which ranges from 0 to the number of locations L. To prevent the same place from being chosen again, the location of the current node is omitted.

$$index = Nmod(L - 1) \tag{2}$$

As soon as a location is produced, the $hash(N)$and $hash(locationlist)$ are broadcast to the network. Broadcasting $hash(N)$ is used to confirm the value of N. After the node initializes IB, a $hash(locationlist)$ is transmitted to ensure that the location list is not changed (Kongahage et al. 2022).

4.6 Short-Range Communication

The prover and verifier transmit data via a short-range communication channel. Mobile devices may communicate across short distances using a variety of methods, including Near Field Communication (NFC) and Bluetooth. The data in figure 2 will be sent by the prover to the verifier.

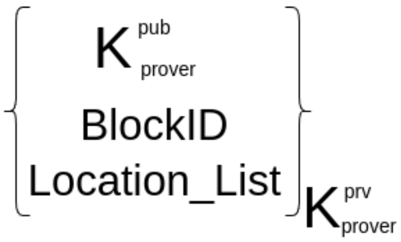

Figure 2: Data sent from Prover to verifier

The prover is uniquely identified using the $K^{\text{pub}}_{\text{prover}}$. To make it tamper proof, the data is signed using $K^{\text{prv}}_{\text{prover}}$. The hash of the IB corresponding to the produced location is called blockId, the unique block identifier. The following crucial verifications need to be made:

1. Confirm that the node and the verifier are near to one other. By tunneling the short-range packets, two users might pretend to have met (wormhole attack).

2. Confirm that the node is indeed a part of the network The prover and availability of the necessary data in the network may be confirmed using the K^{pub} broadcast sent by the node at the first block construction.

3. Check the prover's signature. In order to verify the user's identity and ensure that data is not altered while being transmitted, $K^{\text{prv}}_{\text{prover}}$ signs the data.

4. Confirm the place that was chosen at random. Check to see if the user's broadcast $hash(N)$ value is produced from the IB ticket list.

5. Confirm that the location list hasn't been changed and the order of locations are preserved. To ensure that there have been no modifications made to the location list, it is verified.

6. $index = NMod(Len(locationlist)$-1) and $locationcurrent == locationlist[index]$ can be used to verify location

The prover receives a response, which is the prover's ticket, once the verifier completes the verification. To prevent tampering, the message is signed using the $K_{\text{verifier}}^{\text{prv}}$, guaranteeing non-repudiation. In addition to these checks, there are a number of other security-enhancing checks that may be made, some of which may be implementation-specific. The prover will broadcast the generated ticket to the network. Every node will incorporate the obtained tickets into its ticket pool (Kongahage et al. 2022).

4.7 Leader Selection

As soon as a new block is introduced to the chain, every node participates in the leader selection process and chooses the leader for that block.The leader is chosen based on the available local blockchain ledger.The chosen leader should be unpredictable and random, and is consistent throughout all of the network's nodes.

The tickets from the latest m blocks of the blockchain will be chosen by the nodes in order to choose a leader. The implementation may affect the value m.

Based on the ticket's timestamp, the chosen tickets from each block are placed in chronological order, starting with the earliest. After a validator initializes a ticket, the timestamp that is being considered here is appended.

As seen in equation 3, the random number generator function generates a random number (RN) by utilizing the leader's public key, $K^{\text{pub}}_{\text{n-1}}$, as the seed and the preceding block hash, $H_{\text{n-1}}$. The values of $H_{\text{n-1}}$ and $K^{\text{pub}}_{\text{n-1}}$ are random since the RN generation occurs as soon as a new block is added to the chain.

$$RN = hash(K^{\text{pub}}_{\text{n - 1}} + H_{\text{n - 1}}) \tag{3}$$

$$index = RNmod(L) \tag{4}$$

When choosing the leader for the nth block, an index between 0 and the length of the chosen tickets L may be obtained using equations 4. Using the *index*, a ticket will be selected from the tickets list and the next leader will be K^{pub} , the ticket that was chosen. The leader node itself will discover that it is the next leader as each node in the network goes through this predetermined leader selection procedure. The winning ticket's block will then be selected by the leader from the local block store.

By combining a set of transactions from the transaction pool with the Merkle hash of the transactions $h_{\text{Merkle}}(transactions)$, the leader completes the block, as seen in figure 8.

The hash from the previous block, *previousHash*, is appended and serves as the next block's pointer. The block finalization time is represented by the addition of a timestamp. At last, the hash value is updated. The leader broadcasts the completed block to the network, where every node verifies the block and any available transactions (a process that other blockchains often follow). The new block will be added to their local blockchains after successful verification (Kongahage et al. 2022).

4.8 Forks/Sub-networks

When sub-networks split off and operate independently on their own blockchains, forks may happen. The chains will become inconsistent as a result of this. In a scenario where there are partitions, the partition with fewer nodes will produce fewer tickets than the partition with more nodes. As a result, the partition with fewer nodes will have to wait longer to get the amount of tickets required to start a block. When compared to the blockchain of the division with a higher number of nodes, this will lower the block generation pace and shorten the blockchain's length. The blockchain ledger with the longest length (maximum height) is the one chosen according to the Fork selection rule. As soon as the pace at which criminal users create tickets exceeds that of honest users, this system will become insecure. These users could make a fork with the longest possible length in such a scenario.

5 PoHM Evaluation

In this paper the evaluation is discussed by Kongahage et al. (2022) under three subtopics. Those are Human Mobility, Performance and security. Under this section the results evaluated by the author will be discussed and analyzed.

5.1 Human Mobility

Kongahage et al. (2022) implemented a simulation from p5.js to simulate human mobility in an area of $800mX800m$ area for 30 minutes.
The assumptions made by Kongahage et al. (2022) should be analyzed thoroughly since these assumptions greatly affect a practical implementation.

1. Only direct paths between locations
2. Data exchange time between prover and verifier is negligible
3. Average human speed $2ms^{-1}$
4. No nodes are dropped or added
5. All locations are common to all nodes

Kongahage et al. (2022) was able to implement a simple yet limited implementation of the PoHM algorithm with increasing number of locations. For each number of locations, Kongahage et al. (2022) has taken an increasing number of nodes and have calculated the average number of tickets.

Kongahage et al. (2022) has examined that, when the number of locations increases the number of tickets generated increases.

Also Kongahage et al. (2022) examined that when the number of locations increases the number of tickets verified will be decreased. And also two deadlock conditions were also introduced.

1. $numberofnodes <= numberoflocations$: nodes may have wait indefinitely for another node to visit the same location.
2. Common Location's number of users : If the location is shared by many users there is a hgh chance to get verified

5.2 Performance

Kongahage et al. (2022) implemented a Naive coin Implementation (Conradoqg 2017) by replacing available PoW with PoHM.

Based on the implementation of Kongahage et al. (2022) if there is n number of nodes in the network and X number of tickets generates by a single node within T time a total of $2n^2X + n$ messages will pass through the network. Hence message complexity is $O(n^2)$.

Kongahage et al. (2022) guaranteed that all the nodes maintain identical ledger by outputting the results of the hash values of the first 50 blocks of 10 nodes, hence

Consistency guaranteed.

Kongahage et al. (2022) depicts that the block interval and size affect the throughput/ Transactions per second (TPS). And also TPS reduces when the number of nodes increases.

5.3 Security

Kongahage et al. (2022) has described how the agreement, termination and validity properties maintained. Since honest nodes select same leader consistently, the agreement property maintained.

Since the PoHM always decide next leader when block is added and algorithm termination happens with a final decision, the termination property maintained. A mining node always generate the appended block and it is verified by network and secured by signatures, hence Validity property maintained.

6 Critical Analysis of PoHM

Kongahage et al. (2022) uses human movement tracking to offer a novel consensus method for the blockchain leader selection process. This innovative idea makes blockchain more sustainable. If done correctly, it is also possible to promote and enhance human health and well-being. The drawbacks of the resource-intensive techniques employed in the present algorithms are eliminated by this solution, which suggests human mobility as a trust factor.

The network's reliance on a central authority is decreased because all of its nodes participate in the verification process. Thus, the network's decentralization is strengthened by the algorithm. Furthermore, the choice of leaders is random and fair.

Additionally, when a new block is constructed, incentives are distributed among users who actively participated in the process, and the likelihood of becoming a leader is solely dependent on the user's physical actions.

Moreover, this particular algorithm should not be limited to blockchain technology alone; it can also be utilized in apps and fitness and health trackers. In addition to being advantageous for the end users' health and finances, this is also profitable for the developers. It also serves as inspiration to keep up one's fitness by using smartphone apps and monitors.

However, in order to make this algorithm far more safe, practical, and optimal, it is also important to take into account some of its flaws for future developments. Implementation of the algorithm of Kongahage et al. (2022) is based on five assumptions, and these assumptions could make great impact to a practical implementation of the PoHM algorithm.

Kongahage et al. (2022) has assumed that there will no overlaps of paths between locations, which simply means that locations are directly connected. But in real world this scenario could not be true, hence actions must be taken to mitigate the flaws occur due to unexpected situations. Also the assumption which mentions about negligible data communication time between user nodes is also not true in real world. These two issues can be identified in the following scenario.

If someone with the wrong location(person A) arrives at a another location,where there is already a person (person B) with right location, since they do not there identity the short-range communication starts. Kongahage et al. (2022) already suggested that there should be location verification while the communication happening, person

A could be identified as an invalid user (Since location of person A is invalid). But if the person B needs to verify, it happens successfully because person B is on the right location. If the latter happens first while the short range communication, this causes unfair advantage for the person B.

Therefore as a suggestion, before validating other node, the verifier node itself should be verified against the current location to lock or unlock the verification ability.

Kongahage et al. (2022) has also assumed that no node will be dropped during the implementation process. But in a practical scenario this could be falsified. The already mentioned deadlock in section 4 could occur due to this droppings of nodes and cause deadlock through the system or a subsystem.

Another misuse of the algorithm is usage of transport services. If a node uses a transport service like cars or buses, this causes an unfair advantage for such user. And those kinds of users tend to generate more tickets than other nodes.

And the research has explained what will happen if an odd number of nodes come to a same location. Even number of nodes will perform the verification process but the odd one will not be able to verify even if the user arrives at the location. This may exhaust such users and they may tend not to use this proposed application. Not to mention this also causes humans to participate in unnatural mobility patterns, which could be a time waste and useless.

The performance evaluation of the research of Kongahage et al. (2022) already depicted the scalability of such system decreases against the number of node population increased. Therefore a need of a more optimized mechanism arises. But it is important to understand that this issue already occurs in other algorithms.

The average number of tickets issued decreases as the number of locations increased, according to the Kongahage et al. (2022). But Kongahage et al. (2022) has not considered nor mentioned about the distances/ average distance among locations and the user nodes. There is a possibility that the average number of tickets issued could be increase (or be constant) against the locations, if the distances/ average distance among the locations is low. There more evaluation results should be taken with the addition of a new parameter, distance between nodes.

Also one of the most important flaw that need to be considered and addressed is the the creation of sub-networks or forks. New blockchain networks could be created according to geographical differences in different locations. Malicious attackers or even honest nodes in the network could create such network. Since the Fork resolution rule picks the highest/ longest chain, there could be a biased nature in the network for the powerful sub network. Mohammadi & Rabieinejad (2020) has researched on how to predict forks in blockchains with the use of Machine Learning. A possible answer for this problem is implementing a dynamic point based mechanism for the ticket creation. The value of the ticket point may increase or decrease in accordance to the size of the sub-network, providing fair opportunities for all sub-networks to participate in block creation phase.

7 Conclusion and Future Work

In this literature review, background of the blockchains, different types of Blockchain consensus algorithms,the use of AI in blockchain, sustainability of blockchains and also the new PoHM Algorithm developed by Kongahage et al. (2022) was discussed and critically analyzed. We have found out that this human mobility could cause great positive impact on sustainability and also for human health. Also some of the impractical issues of this algorithms was also discussed. As mentioned in section 6 odd arrival issue should be mitigated by providing some facility or upgrading the consisting verification mechanism. And also to mitigate abnormal human mobility patterns, the user node should be able to select preferred locations or a Machine learning algorithm can be implemented to identify nearby locations. And another important thing to be considered is the commonality of locations among user nodes. Also the the fork issues addressed in section 6 should be mitigated. A dynamic point based mechanism can be introduced to the tickets to increase or decrease the total values of tickets in each fork networks, hence providing each sub-networks an equal opportunity to participate in block creation phase.

References

Aluko, O. & Kolonin, A. (2021), ‘Proof-of-reputation: An alternative consensus mechanism for blockchain systems’, *International Journal of Network Security Its Applications* **13**.

Badawi, E. & Jourdan, G. V. (2020), ‘Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review’, *IEEE Access* **8**. nikn attaks tikk.

Bentov, I., Lee, C., Mizrahi, A. & Rosenfeld, M. (2014), ‘Proof of activity: Extending bitcoin’s proof of work via proof of stake’, *Cryptology ePrint Archive* **452**.

Conradoqg (2017), ‘A cryptocurrency implementation in less than 1500 lines of code’, `https://github.com/conradoqg/naivecoin`. Accessed: 17/02/2024.

De Vries, A. (2023), ‘Cryptocurrencies on the road to sustainability: Ethereum paving the way for bitcoin’, *Patterns* **4**. why eth good¡br/¿but how it cant win...

Dziembowski, S., Faust, S., Kolmogorov, V. & Pietrzak, K. (2015), Proofs of space, *in* ‘Annual Cryptology Conference’, Vol. 9216. ref for PoW get it¡br/¿maths part is hard.

Fu, X., Wang, H. & Shi, P. (2021), ‘A survey of blockchain consensus algorithms: mechanism, design and applications’, *Science China Information Sciences* **64**.

Gallersdörfer, U., Klaaßen, L. & Stoll, C. (2020), ‘Energy consumption of cryptocurrencies beyond bitcoin’, *Joule* **4**.

Ghosh, A., Gupta, S., Dua, A. & Kumar, N. (2020), ‘Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects’, *Journal of Network and Computer Applications* **163**.

Goodkind, A. L., Jones, B. A. & Berrens, R. P. (2020), ‘Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining’, *Energy Research and Social Science* **59**. mining locations on US.

Gundaboina, L., Badotra, S., Bhatia, T. K., Sharma, K., Mehmood, G., Fayaz, M. & Khan, I. U. (2022), ‘Mining cryptocurrency-based security using renewable energy as source’, *Security and Communication Networks* **2022**.

Huang, J., Kong, L., Dai, H. N., Ding, W., Cheng, L., Chen, G., Jin, X. & Zeng, P. (2020), ‘Blockchain-based mobile crowd sensing in industrial systems’, *IEEE Transactions on Industrial Informatics* **16**. MCS¡br/¿BMCS¡br/¿why MCS bad¡br/¿blockchain in MCS.

Jayawardhana, A. & Colombage, S. (2020), *Does blockchain technology drive sustainability? An exploratory review*, Vol. 15, Emerald Publishing Limited, pp. 17–42.

Karger, E., Jagals, M. & Ahlemann, F. (2021), ‘Blockchain for smart mobility-literature review and future research agenda’, *Sustainability (Switzerland)* **13**.

Khan, D., Jung, L. T. & Hashmani, M. A. (2021), ‘Proof-of-review: A review based consensus protocol for blockchain application’, *International Journal of Advanced Computer Science and Applications* **12**. look explan of algo and attack types.

Kongahage, M., de Zoysa, D. & Sayakkara, D. (2022), ‘Proof of human mobility: A novel permissionless consensus algorithm for blockchains, based on human mobility’.

Kwon, Y., Liu, J., Kim, M., Song, D. & Kim, Y. (2019), Impossibility of full decentralization in permissionless blockchains, *in* ‘Proceedings of the 1st ACM Conference on Advances in Financial Technologies’. Importance of decentral.

Lin, I. C. & Liao, T. C. (2017), ‘A survey of blockchain security issues and challenges’, *International Journal of Network Security* **19**. Forks ...

Mohammadi, S. & Rabieinejad, E. (2020), ‘Prediction forks in the blockchain using machine learning’.

Wagner, K., Keller, T. & Seiler, R. (2019), A comparative analysis of cryptocurrency consensus algorithms, *in* ‘Proceedings of the 16th International Conference on Applied Computing 2019’. comparison 1k.

Warmke, C. (2024), ‘What is bitcoin’, *Inquiry* **67**(1), 25–67.

Wüst, K. & Gervais, A. (2017), ‘Do you need a blockchain?’, *IACR Cryptology ePrint Archive* .

Zhang, Z., Song, X., Liu, L., Yin, J., Wang, Y. & Lan, D. (2021), ‘Recent advances in blockchain and artificial intelligence integration: Feasibility analysis, research issues, applications, challenges, and future work’, *Security and Communication Networks* **2021**.

Zheng, Z., Xie, S., Dai, H. N., Chen, X. & Wang, H. (2018), ‘Blockchain challenges and opportunities: A survey’, *International Journal of Web and Grid Services* **14**.

Index