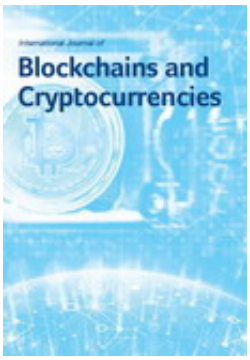
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Blockchains and Cryptocurrencies

ISSN online: 2516-6433 - ISSN print: 2516-6425
https://www.inderscience.com/ijbc

Missa: a regional approach to maintain validity

Mohamed Ikbal Nacer, Simant Prakoonwit, Edmond Prakash

DOI: 10.1504/IJBC.2023.10056797

Article History:

Received:	06 May 2022
Last revised:	02 August 2022
Accepted:	03 August 2022
Published online:	21 June 2023

Missa: a regional approach to maintain validity

Mohamed Ikbal Nacer* and Simant Prakoonwit

Department of Creative Technology,
University of Bournemouth,
Dorset, UK
Email: mnacer@bournemouth.ac.uk
Email: sprakoonwit@bournemouth.ac.uk
*Corresponding author

Edmond Prakash

Cardiff School of Technologies,
Llandaff Campus,
A Block, Cardiff CF5 2YB, UK
Email: eprakash@gmail.com

Abstract: Blockchain is a new technique developed to eliminate central management of information by dividing maintenance between validators interested in participating for an expected reward. Unlike previous work, this invested in the practical impossibility of dealing with a large number of maintainers who may be business owners expecting a reward or aiming to foster the ecosystem. Inspired by the proverb "solidarity is not an act of charity, but mutual aid between forces fighting for the same goal." This work introduces Missa, which is a way to foster trust between different maintainers and the platform by exchanging valuable data structures to provide a new approach to maintaining ledger validity in a fast, reliable, and secure manner. The solution was evaluated in terms of security discussion, environmental modelling, formal study of important components, and conceptual comparison. Finally, an actor model implementation, network simulation and unit tests were demonstrated.

Keywords: blockchain; artificial intelligence; graph theory; consensus; proof of work; PoW; proof of stake; PoS; Byzantine fault tolerance; BFT.

Reference to this paper should be made as follows: Nacer, M.I., Prakoonwit, S. and Prakash, E. (2023) 'Missa: a regional approach to maintain validity', *Int. J. Blockchains and Cryptocurrencies*, Vol. 4, No. 1, pp.26–64.

Biographical notes: Mohamed Ikbal Nacer is a PhD student at the Bournemouth University. He holds a Degree in Mathematics and Computer Science from the Abdelhamid Mehri University of Constantine 2 – Constantine. He also holds a Master's in Mathematics and Computer Science from the same university. He benefited from a short industrial experience in fields such as IoT, automotive and web development.

Simant Prakoonwit won the British Government's Colombo Plan Scholarship to study in Britain. He began research in artificial intelligence (AI)/3D computer vision when studying for an MSc in the Department of Electrical and Electronic Engineering, Imperial College London. He then did a PhD research on AI/3D computer vision, reconstructing 3D objects from X-ray, also at Imperial. Subsequently, he worked as a Post-doctoral Research Assistant in Imperial College's Department of Bioengineering, on 3D computer vision (grant from Home Office, UK). His work can be applied to both security, e.g., airport weapon and bomb scanning, and medical applications. His doctoral and postdoctoral research is patented by Imperial.

Edmond Prakash received his PhD in Visualisation from Indian Institute of Science. He is currently the Director of the Research Centre for Creative Technologies, University for the Creative Arts, UK. He leads research in the underpinning technologies in the design, development and deployment of the scalable metaverse as a Professor in Metaverse Technology. He served as the Founding Chair of the Computer Science Department at Leeds Trinity University, UK and was a Professor and Research Dean for the Cardiff School of Technologies, Wales, UK. He has supervised ten PhD students and authored more than 200 peer-reviewed papers.

1 Introduction

The blockchain as presented in the Bitcoin report (Nakamoto and Bitcoin, 2020) aims to secure a tamper-proof and tamper-resistant ledger. It was later explored as a way to maintain the validity of a ledger through many consensus techniques. The transaction is the user's initiative element, it contains an exchange object, which can be a UTXO, balance information or a different modelled token and verified signature with user's pair keys (Tuzi, 2018). A list of transactions will be hashed using Merkel tree to then be injected into a block containing other information and especially the nonce number. It will be used to generate unique hash value through random search to represent high cost of malicious activities. Banks play the role of mediator between the depositor and the borrower and have developed massively in recent years. The use of technology and in particular blockchain can be another way to reduce the bureaucratic burden of the financial institution. The blockchain differentiates between two types of users, which are the simple user who exchanges values and the maintainer who validates these values. Proficiency is the key element among validators to ensure validity either through stakeholder decision or miners in the case of Bitcoin models. Many very descriptive works have been provided in the literature. The book in (Goundar, 2020) provided an advanced discussion such as a literature review (Goundar et al., 2021b), in which impactful articles were identified and the techniques used were explained and another chapter that discussed the fundamental rights supposed to be provided by blockchain technology.

Khaldun (2015) introduced sociology to the world and stated that the state has always been a human choice to maintain justice but questioned that the state itself is a force that acquires power unfairly. The story of an ancient society is summarised in a long road to a sophistication that ends with a huge focus on art before a foreign minority

with the foundational skills comes to take over. Solidarity among people who speak the same language was the key to maintaining the society internally. However, the focus has been on the cultural clash, investing in bureaucracy as an internal issue against solidarity. Kansas City has experienced a large number of crimes involving special areas, into which considerable research has been invested in finding the best tactics for dispersing the police. The solution was found through the use of coupling within graph theory by associating dangerous places with a high number of police comparable to peaceful regions (Gladwell, 2019).

Many social issues related to personal psychology can lead to social punishment, such as mismatch, transparency, and truth bias (Gladwell, 2019). The modelling of the problem can be both probabilistic and deterministic. However, the probabilistic approach, led by the Bayesian network, presents many philosophical problems which exclude it from the field of epistemology (Chandler, 2017). Therefore, Chandler (2017), adopted a deterministic approach called ranking theory to overcome the revision problem with the AGM framework (Delgrande et al., 2018). The ranking theory has not yet solved the problem, but it is a solid way to build a self-adapting system and to solve the problem of prior extrinsically.

Blockchain's goal is to eliminate the foundation of normal human society, which is the state. It will eliminate the force that uses unfair means to enforce bureaucracy, which prevents human civilisation from growing rapidly. The problem of malicious activities can be summed up in the same conflict of nomads with those who are sedentary. The ability of validators to monopolise the system can be seen as the issue of the periodic existence of a foreign minority that possesses the foundational skills. However, graphical analysis of the blockchain ledger has shown many cycles that can be inferred as ways to increase the value of cryptocurrency through a bogus exchange or double-spend events by investing in the longest chain rule. All of these latter issues can be justified or denied based on mismatch, transparency, and truth bias of human psychological interaction. Therefore, it will be difficult and unfair to implement a probabilistic model to deal with these issues. On the other hand, the deterministic approach can be appropriate.

This work imports social behaviour into the system by investing in human nature. It uses a model (Nacer et al., 2021) that initiate the transaction from the receiver side to be a driver of solidarity. This article asks the following question: "if the state has always been a chosen force, why are the bureaucratic institutions not distributed among us?" Specifically, the primary contribution of this work is the following:

1 The introduction of a novel approach to maintain ledger validity and preserve high scalability at the same time.

2 The introduction of the concept model, which can provide a simple, agile and flexible development approach for a dynamic framework.

3 The provision of security and modelised decisions as a network connection instead of a computation component to ensure reliability.

4 A theoretical study has been provided in terms of a security discussion, a formal study of different components, modelling of the operating environment, and a conceptual comparison. Finally, an actor model implementation, network simulation, and unit tests have been demonstrated.

The whole vision of the system is to provide a new web where the user's view of truth is reputable, authentic and part of a regional preference that forces different versions of consistency. The web can be used for any type of value or managed information. Moreover, the modular dynamic growth of the system is based on a conceptual basis to generate a decision based on a network that explores different paths, making regional consistency another term for different objects. Section 2 will provide related work in the literature of different components, in addition to the existing parallel solutions. Section 3 is a motivation. Section 4 will present the different components of the proposed solution. Section 5 is an evaluation of the approach. Section 6 is dedicated to testing, before the paper ends with a future works and conclusions in Sections 7 and 8.

2 Related work

Proof of work (PoW) is an approach that designs a framework where a sibling attack cannot be practically performed. The hash power increases massively as the requirement for the leading zero increases. The ledger is built through competency to generate the longest chain. Many pieces of research have studied its distributed execution. For example, Eyal and Sirer (2014) studied the mining strategy, in which the race led to collisions within the system called pools. Each pool executes a specific protocol to divide the search space among the participants (Nakamoto and Bitcoin, 2020). Other selfish mining strategies that have been explored, such as block withholding (Wu et al., 2019a), lie in wait (Vyas and Lunagaria, 2014), and pool-hopping (Belotti et al., 2018). Liao and Katz (2017) investigated Bitcoin ledger bribes using a whale transaction (WT), which represents a high validation fee to trick the validator into aiming to fork. Many variants of Bitcoin PoW that invest either in compute-bound or memory-bound have been proposed, such as Wu et al. (2019b). PoW suffers from high resource consumption, subject to 50% attacks (Shalini and Santhi, 2019), monopoly and double-spend (Zhang and Lee, 2019). The work in Goundar et al. (2021a) provided a taxonomy on the current blockchain platform, the factors behind its success, the companies that use the technology, and its application across different domains.

Many proposals have been published to improve upon Bitcoin implementation, such as improvised Bitcoin-NG (Das, 2021) or subchains (Rizun, 2016). For example, Das (2021) focused on increasing throughput and fairness but the approach was prone to flooding attack (Wang et al., 2019a) besides an incentive consideration (Yin et al., 2018a). In addition, many proposals have invested in the random delayer such as proof of elapsed time (PoeT) through the use of Intel hardware (Kumar et al., 2019). Proof of space (PoSp) is achieved by switching from the dedication of computation resources to the sharing of disk space (Tang et al., 2021). Proof of useful work (PoUW) (Loe and Quaglia, 2018) is achieved by ensuring that resources have been used to solve a useful task. However, the different implementations have been criticised due to security requirements. PoeT suffers from the lack of global control over the clock and PoSp suffers from the expected high level of resources required. The PoUW protocol suffers from the lack of incentive, unmet consensus requirements, and the impracticality of some proposals. Moreover, improvised Bitcoin-NG requires some synchrony that exposes the system to a DoS attack, and faces issues such as correctness, latency, and targeting through undermining the leader.

Byzantine fault tolerance (BFT) was introduced by Lamport (Gramoli, 2020) to solve the problem of the order of events. It was followed by Paxos, which came up with a solution to fault tolerance. Castro et al. (Haldimann et al., 2021) proposed the practical BFT (PBFT) by extending Paxos to crash failures. It secures normal operations in a partial synchronisation mode but with very high message complexity, it has been followed by many proposals to optimise its execution, such as Zyzzyva (Sohrabi and Tari, 2020). Therefore, its suitability in the realm of permissionless consensus (Gramoli, 2020) has been widely discussed. Hotstuff (Yin et al., 2018a), implemented in Libera, aims to optimise the throughput by using BFT pipelining but this has introduced a longer chain of causal links between initiation and finality. Streamlet (Chan and Shi, 2020) aims to increase fairness through the rotation of leaders. It has decreased the number of messages but still suffers from $O(N^3)$ of communication costs applied at three rounds. Malkhi et al. (2019) introduced the flexible BFT which develops a dynamic quorum and addresses the issue of alive-but-corrupt members. Nevertheless, due to the high complexity of messages with bandwidth restrictions, the adoption of BFT in permissionless blockchain has been met with skepticism. Thus, most BFT approaches have been proposed for use in a permissioned environment such as Stathakopoulou et al. (2019).

Proof of stake (PoS) (Kim et al., 2018) is a solution that attempts to remedy the PoW consumption of resources. The incentive for valid participation lies in the fact that stakeholders will be interested in the ledger's validity, in which the validator selection process must follow a random algorithm such as follow-the-Satoshi, coin-age, PoW random selection, or validator random selection. Many proposals in the cryptocurrency sector incorporate PoS and BFT as a voting mechanism to finalise a block, such as Tendermint (Buchman, 2016), which uses BFT-spinning to manage throughput, or Ouroboros-BFT (Kiayias and Russell, 2018). Chained PoS is based on a combination of PoW and PoS by securing a large number of participants via PoW and then switching to PoS. The delegated PoS (Fan and Chai, 2018) is based on a community selection of validators, it is more closely associated in its philosophy with the delegate BFT. PoS, in its philosophical context, suffers from monopoly and mining cartels because an alternative chain is easy to generate (Zamani et al., 2018). However, the various hybrid solutions have not shown any advantages but have inherited the disadvantages of each technique at each level.

Tangle (Silvano and Marcelino, 2020) is a proposal to solve the high fees within an open blockchain system. The solution offers a directed acyclic graph. The submission rate is the factor that eliminates manipulation with the use of a small hashcash PoW puzzle on the user side. However, Tangle suffers from high consumption of distributed resources, which IoT devices may not be able to manage (Wang et al., 2019b), is prone to splitting attacks (Silvano and Marcelino, 2020; Bu et al., 2019), 34% attack (Sayeed and Marco-Gisbert, 2019), and monopoly. G-IOTA (Wang et al., 2019b) is another selection algorithm used to overcome the left behind tips.

Peer-to-peer implementation is the basis of blockchain dissemination of information through the propagation of transactions or blocks. The topology of the network above in which the system is functioning is very important for its security. Network discovery is the first step for the new joiner, in which IOTA uses peers' gossip to forward neighbors' tables and Bitcoin uses DNS servers to extract seeds. On the other hand, a proposal such as Kademlia suffers from a lack of proof of its real performance (Dotan et al., 2021). However, restrictions on the inbound and outbound number of connections lead

to forking when it is correlated with a high number of miners. Moreover, DNS poisoning (Al-Mashhadi and Manickam, 2020) or RBG hijack (Awe et al., 2020) may undermine the network. Transaction propagation occurs through gossiping (Nencha, 2021) or the use of the Geth protocol (Delgrande et al., 2018). Finally, block propagation is through the use of protocols such as weak block (Roy et al., 2018), graphene (Ozisik et al., 2019), velocity (Chawla et al., 2019), high and low compact encoded block, or stratum (Recabarren and Carbunar, 2017). Nevertheless, the network lacks a complete incentive that forces cooperation due to the functioning of the tragedy of commons embedded in the system, in which miners are not interested in clients' satisfaction but selfish gain. Moreover, the geographic concentration of miners can be the cause of an RBG hijack, in which a study has shown that removing 50% of a network's hash power is possible by eliminating fewer than 100 gateways (Saad et al., 2020).

AGM is a framework that has been implemented to study epistemological theory using the qualitative approach of formal logic. The system has three functions that describe its growth: expansion, contraction, and revision (Kern-Isberner et al., 2019). A revision will address rules that can be misunderstood to generate an unpredictable sequence of actions (Chandler, 2017). Much work has been done to manage uncertainty above this domain, such as fuzzy logic (Zadeh and Aliev, 2018), possibility theory (Mei, 2019), and plausibility (Lai, 2019). However, based on Gödel's incompleteness theorem, it is impossible to achieve infinite learning using the available formal logic because any system depends on an external assumption made by ourselves in the first place (Iacona, 2021). The Bayesian network was, for a time, an alternative to managing uncertainty, but numerous epistemological refutations have been posted in the literature, such as Chandler (2017). In the Bayesian ideology, it is irrational to be certain, there is no suspension of belief, it can describe content with many representations, and there is no support for iterative learning. Thus, Chandler (2017) proposed the ranking theory as a deterministic approach to representing the dynamics of belief. Following is a formal representation of its conditional function and negative ranking:

Let R be a negative ranking function for algebra, $a \in B$, $x \in R^*$, and $R(b)$, for b, $b \in B$, R is a ranking function from b into $R^* = R^+ \cup \infty$.

$$R(B) = 0,\ R(\emptyset) = \infty$$
$$R(a \cup b) = \min(R(a), R(b))$$
$$R(a) = 0 \text{ or } R(\neg a) = 0 \text{ or both}$$
$$R(\cup b) = \min(R(b))$$

Chandler (2017) proposed a conditional function, but was criticised by Shoney for relevance and proposed a modification for evidence lead tracking. The following is the function proposed by Shoney: Let R be a negative ranking function for algebra B, where $b \in B$, $x \in R^*$, and $R(b)$, $R(\neg b) < \infty$.

$$f(x) = \begin{cases} R(a \mid b) - y & \text{if } (a \in b) \\ R(a \mid \neg b) + x - y & \text{if } (a \in \neg b) \end{cases} \quad \text{where } = \{\min = R(b) \mid x\}$$

Community detection has been one of the main areas of research in a social network in which many greedy search algorithms have been proposed. A tree is a special data structure that is useful in many applied fields. It is a restricted graph that is directed and does not contain cycles. Many algorithms have been proposed to process the learning of

trees. However, many questions have been raised based on the philosophical question of when to stop, in which post-pruning and overfitting, with some randomness, were the two choices (Chourasia, 2013). The splitting of a node, in which a distance measure has been incorporated or an impurity function has been evaluated, has also been widely discussed. One of many implementations is FastXml (Prabhu and Varma, 2014), which is a ranking algorithm that builds a random forest, taking into account the division of a node with the use of SVM (Yan and Jia, 2018) and a stop condition based on entropy gain.

3 Motivation

The motivation for this proposal is to address the bureaucratic workload of government by providing a social science-inspired algorithm to construct a new mode of belief as an adaptable internal decision-making system as users control its growth based on their needs provided by the concept manager, who are validators. The basic proposition is to provide a way to apply the same techniques that humans apply socially to gain power or deter against threads, which are reputation building and destruction. This work provides a new way to reinforce the belief in the distributed system named the concept model to be coupled with a sociological algorithm to act as a means of reputation building by providing new concepts to be used by customers or reputation destruction to deter malicious users. it assumes working on a two-layer network, one dedicated to validators and the second to customer communities. Moreover, we affirm that there is no need for global consistency but for intersecting interests within an overlapping regional consistency. Nodes will be coordinated by Missa to act competitively. Figure 1 is a demonstration of the system's vision. The solution provided in this work is a way to respond to philosophical limits by playing on the following principles:

1 Increase efficiency of the system by lower the time of finality.
2 Provide a novel artificial intelligence method to be the background of a world machine.
3 Respond to the legal requirement on the personal and state level.
4 Provide a new model to conceptualise the distributed system.
5 Provide a solution that trade off between real world requirements and fast propagation, treatments, and global decision on a transaction.

4 Missa

4.1 Data structure

Profiling is an approach to measure the subject's tendency, risk, and normal behaviour that can be targeted or evaluated based on it. It can be as well the modulisation of the object of belief, in which inter-regional concepts can build an inferential belief. The belief as an object that does depend on properties and relations must not be taken in the relative sense to a concept but to a distributed entity itself. This section will introduce

the management of belief within the peer, in which the different data structures that have been implemented will be demonstrated and analysed. Classes are demonstrated in Figure 2.

Figure 1 Modular flow (see online version for colours)

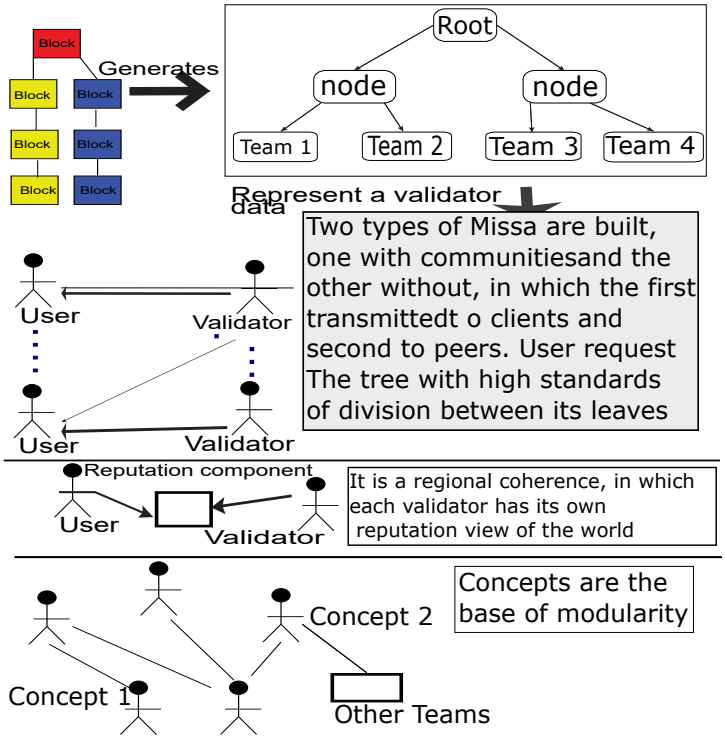
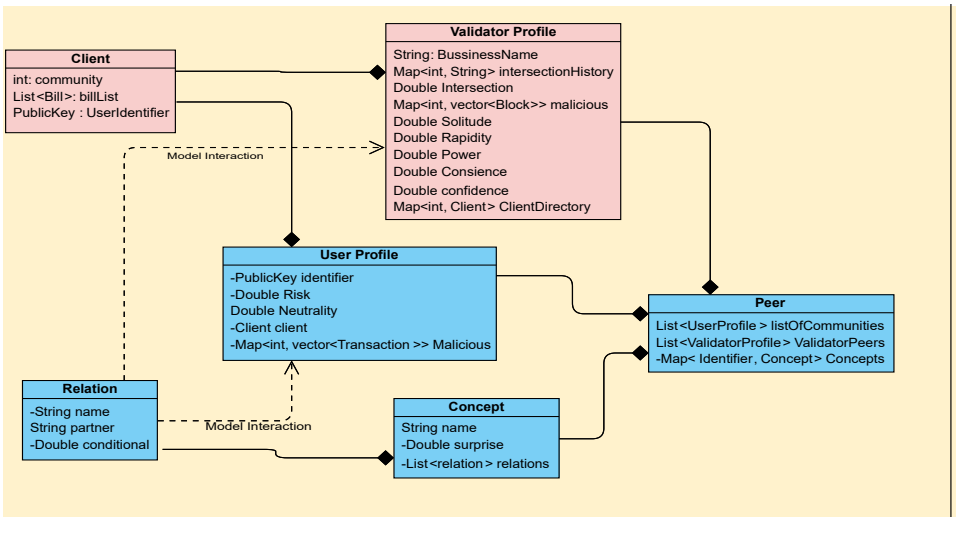


Figure 2 Flow of data (see online version for colours)



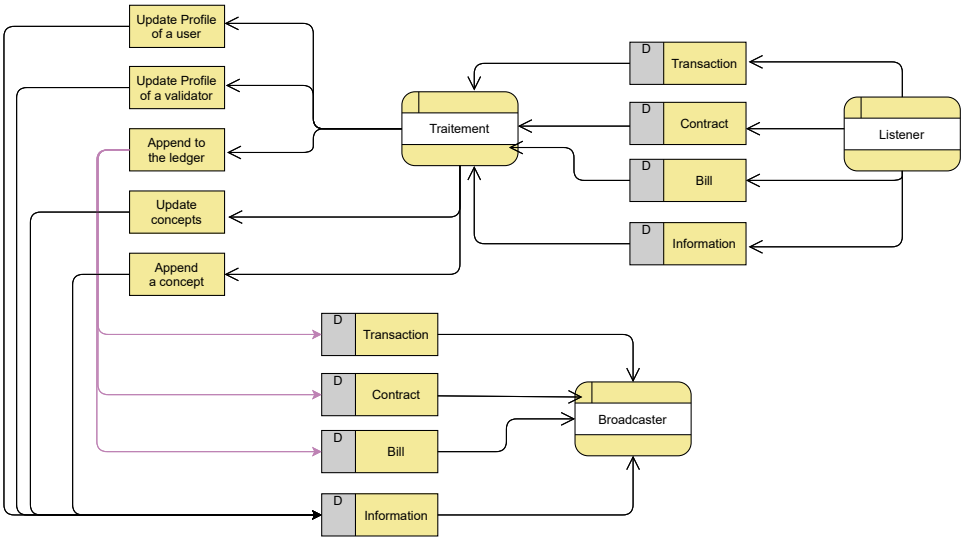
The user profile contains an identity which is a public key. Risk represents disbelief in a connection, and it is bound to zero to be its suspension. Neutrality means the opposite of risk, which is a list of evidence of malicious activities. The risk is derived in terms of ponderations; in other words, each data point contributes differently to the risk metric. These ponderations must be constantly updated by an expert in the field to be up to standard. In addition, the client class contains a community number identifier and a list of bills.

The validator profile contains a business number, which provides a good measure of confidence for the user. History represents different peers that have a high exchange rate with the validator. Intersection represents the regional number of intersections. The client directory represents all the clients registered with the validators. The remainder is variables related to the validator's physical device. Relations between peers are managed through concepts, which have a name, a surprise factor that represents the mean of the relational values, and a list of relations. The relation class contains a partner name, a name or reference, and a conditional value handled with Shoney conditionality.

Missa will be presented in a node and built recursively. It contains a list of validators who have reached the node and a logistic map that assesses the level of randomness in the choice. Concepts represent the instances of concepts managed between validators. Communities represent the communities detected via the Louvain algorithm (Singh and Garg, 2021) which will only be applied to leaves of Missa.

The peer in Figure 2 comprises three different lists of entities: concepts, a validator profile, and a user profile. The concept comprises many relationships that manage interaction with validators or users. A validator profile contains a list of clients that will be modelled in terms of communities, and a user profile contains a client object.

Figure 3 Flow of data (see online version for colours)



4.2 Data flow of Missa

At Missa level in Figure 3, the data structure is seen as an action-reaction set. The listening process will deserialise the data to be formed in terms of transaction, contract, bill or information. It will be passed to the processing process and result in different actions to be assigned to different entities, which update the profile of the user or validators, add the ledger, update the concept or add a new one. Finally, the data structure will be passed to the broadcast component to broadcast the information to the peers.

4.3 Reputation-based network

Building belief in the peer arrives through the management of the reputation with the existing region besides the value of the exchange itself. Harm is disbelief within an entity. The connection side will be managed continuously through Algorithms 1 and 2, which update belief in relationships, before modifying the surprise in the concept through Shoney conditional function. First, Algorithm 1 receives a user profile and the vector of transactions. The user will count the number of duplications, inconsistencies, and forbidden actions. Punishment will be relative to the number of users in the initiator's community. The result will be evidence of malicious behaviour to make the receiver unlink the binding with it as the disbelief in this entity turns out to be harmful.

1 Duplication: Two transactions that contain the same sequential number and/or the same coins.

2 Inconsistency: A transaction received from a user in another region that does not stand this rule: $Sequential(i) = Sequential(i-1) + 1$.

3 Forbidden: A transaction with coins which have been used, not possessed, or $Sequential(i) < Sequential(i-1) + 1$.

Algorithm 2 updates the validator profile by checking in the DNS ledger whether the attached block has been registered as malicious through verifying content and identity. RelevantIntersection is a variable that proportionately describes the expected level of intersection. it will be multiplied by the number of validators and proven malicious activities. Thus, the platform community growth has high relevance to punishment. Moreover, it will be harder for highly intersected nodes compared to others to participate in any misbehaviour.

Algorithm 2 manages validators and ponderate profiles according to three criteria:

1 Doggedness: The act of resubmitting a block that contains proven malicious activity.

2 Overlooking: The action of distributing user data containing prohibited transactions for validation.

3 Region intersection: This represents the number of intersections in the regions across which the subject validator operates.

Algorithm 1 Update user

Input: profile, transactions
Output: profile
1 $dup \leftarrow searchDuplicate(transactions)$
2 $inCon \leftarrow countInconsistency(transactions)$
3 $forb \leftarrow countForbidden(transactions)$
4 $CommSize \leftarrow CommunitySize(Profile)$
5 $Evidence \leftarrow Multiply(Add(dup, inCon, forb), CommSize)$
6 $updateRisk(Evidence, profile)$

Algorithm 2 Update validator

Input: profile, block
Output: profile
1 $intersectionFactor \leftarrow deduct(1.1, Divide$
$(intersection(profile), MAXintersection))$
2 **if** $BlockNotValid(block) = true$ **then**
3 **if** $checkDoggedness(profile, block)$ **then**
4 $Evidence \leftarrow Multilply(intersectionFactor,$
$Multilply(doggedness, size(validators)))$
5 **else**
6 **if** $Overlooked(block)$ **then**
7 $Evidence \leftarrow Multilply(intersectionFactor,\ size(validators))$
8 **else**
9 $Inform(validatorProfile, block)$
10 $updateRisk(Evidence, profile)$

4.4 Node splitting

The usual communities expected to be detected within a social network are out of date. However, the splitting of nodes is usually based on a distance metric, in which a goal of extracting the distribution to overfit or adding randomness to suppress an expected outcome are the two options. In addition, a behaviour tree that aims to model the system fails to handle dynamic iterative beliefs. Thus, Missa is a dynamic solution with injected social behaviour that turns decisions into a network to overcome previous philosophical limitations. Concepts such as ‘shop’, ‘sun’ or ‘taste’ can, themselves, be transformed into relations and studied in terms of interactions such as ‘taste’, ‘hurt’ or ‘credibility’ to build a complex sequence of the infinite world of worlds.

4.5 Relevance map and set prior belief

Interaction must take into account the transmission and reception from each entity separately. Each direction must guarantee ‘no noisy data’, which is generally considered in a probabilistic approach. The goal of Algorithm 3 is to build concepts and a ranked list of exchanges. In line 9, the splitting of the data into sent and received is combined in 10 based on the mean value. From 11 to 16, each interaction with a validator is represented in terms of a concept in which two relations will be built to model direction. The value of surprise on the relational level is relevant to the exchanged value minus

the value of malicious activities multiplied by the number of validators. The partner name is the peer's name. OutName, InName, and ConceptName represent the names of outgoing relations, incoming relations, and concept respectively, in which description will allow building more complex beliefs above them.

Algorithm 3 Rank

Input: $data, conceptName, OutName, InName,\ DNSLedger, validator$
Output: $sorted, concepts$
procedure CONDITIONAL($DNS_{Ledger}, Validator$)
    $prior \leftarrow valueMalicious(DNSLedger)$
    $value \leftarrow valueExchange(validator)$
    $return\ Divide(Multiply(value–(Multiply\ (prior, validatorSize))), prior)$
$validators, received, sent \leftarrow splitdata(data, validator)$
sorted ← BasedOnMean(received,sent)
received before sorting it
for $validator\ in\ validators$ **do**
    $initiate(concept, conceptName)$
    $initiate(relations, InName, OutName)$
    $set(relations, validator)$
    $Conditional(relations, Conditional(DSNLedger,$
    $(sent(or)received), Size(validators), validator))$
    $set(relations, concept)$
    $setSurprise(concept, mean(sorted, validator))$

Algorithm 4 Team division

Input: $data, conceptName, OutName, InName,\ DNSLedger, validator$
Output: $teams, concepts$
$Sorted1, concepts1 \leftarrow Rank(data, conceptName,$
$OutName, InName, DNSLedger, validator)$
$set(removeHigherRanked(Sorted1), FirstPartner)$
$Sorted2, concepts2 \leftarrow Rank(data, conceptName,$
$OutName, InName, DNSLedger, FirstPartner)$
$Remove(Sorted2, validator)$
for $element\ in\ sorted1$ **do**
    $value1, value2 \leftarrow extractSurprise(concepts1,\ concepts2)$
    if $value1 > value2$ **then**
        $append(element, left)$
    else
        $append(element, right)$
$Add(validator, left),\ Add(firstPartner, right)$
$return\ setTeam(team, [left, right])$

4.6 Relevance map and set prior belief

The centralisation of a member within a society is an approach to characterise his behaviour leading to the maximisation of the gain to be conditioned by his relationships. However, each set of entities is an interchange region with gates to another parallel,

intersection, or container region. The gates ensure the absence of dominance or build advanced knowledge.

The goal of Algorithm 4 is to build teams related to the trust from each peer to another based on the recorded ledger of malicious activities (the DNSLedger) and the portion of managed data. After calling rank at 4 and 6 to extract rank for the validator and its first competitor, 8–13 is implemented to assess to which side the trust is higher for validators to be associated.

4.7 Tree building

An entity can build, with an ensemble of heterogeneous entities, a world upon different concepts. Many functioning worlds may be impossible, which means inconsistency, but due to the lack of evidence, because there is no complete existence of characterised entities, the world may flourish. Entities must ensure their knowledge is such that their world is consistent, and trust can be increased in it. In this way, there are financial, social, or biological gains to each entity where harm does not exist. Spotting and eliminating the malicious activities within the world lie in the members' instincts, driven by gains. The members that constitute a world conceptual community are defined by the characteristics of the world itself; consequently, a stopping condition is a very important element from a creational perspective.

Algorithm 5 Build tree

Input: $node, data, conceptName, OutName, InName,$
$DNSLedger, validator, worldSize$
Output: $tree$
procedure SETTONODE($node, data, concepts, team,\ compititorTeam, direction$)
if $Size(teams) <= worldSize$ **then**
    $setIntersection(Concepts)$
    $setConscience(Concepts)$
    $setCommunities(Louvain(data))$
else
    $filterOutCompetitorTeam(transactions)$
    $setNode(concepts)$
    $buildTree(data, conceptName, OutName,$
    $InName, DNSLedger, validator, worldSize)$
$teams, concepts \leftarrow Teamdivision(data, conceptName,$
$OutName, InName, DNSLedger, validator)$
$setNode(concepts)$
$setToNode(node, data, concepts, team.get(0)(\text{``}team\text{''}),$
$team.get(1)(\text{``}CompetitorTeam\text{''}), \text{``}left\text{''})$
$setToNode(node, data, concepts, team.get(1)(\text{``}team\text{''}),$
$team.get(0)(\text{``}CompetitorTeam\text{''}), \text{``}right\text{''})$

4.8 Stopping condition

An organisation driven by Missa must have a stopping condition defined by the minimum number of components that build a world. The recursive construction of Missa will be maintained until the basic world number is reached. The gates between worlds are not organised entities, but they are treated as parts of the regional system based on their exchanged value extracted from the data held by the validator. Algorithm 5 represents the recursive building. In the end, a sequence of leaves will be constructed, in which the further to the right of the main validator, the level of competence rises. However, at the community level, this means higher reputation destruction.

4.9 Surf Missa

The usual trick of society when a chosen force tries to apply a harmful interaction such as a high tax is to invest in a new chosen force. The distribution of force allows each entity to nest a client's directory, but if an entity acts in a harmful way with a member that has proof of its behaviour, it decreases trust within that entity, which will drive the R up in the logistic map, driving the algorithm to act within its limits, and then periodically or chaotically to involve other forces that might be interested in overtaking the environment. Algorithm 6 describes the stage when Missa leads the client to defend itself against malicious activities by involving other validators to increase the rate of deterrence.

Algorithm 6 Surf Missa

Input: $node, Validator, depth, R, step$
Output: $Validators, Communities$
$set(step, R/depth)$ if R!=0
if $round(step) == 0$ **then**
  $nodeSon \leftarrow nextNode(node, Validator, R)$
else
  if $round(step) == 1$ **then**
    $nodeSon \leftarrow nextNode(node, Validator, R,\ false)$
  else
    $R \leftarrow floorUpTo(4, step)$
    $value \leftarrow LogisticMap(R, Number)$
    if $value < 0.5$ **then**
      $nodeSon \leftarrow GetRight(tree)$
    else
      $nodeSon \leftarrow GetLeft(tree)$
if $nodeSon\ is\ null$ **then**
  $return\ node$
$step \leftarrow Add(step, Divide(R, depth)))$
$step \leftarrow Add(step, Divide(R, depth)))$
$surfMissa(nodeSon, Validator, depth, R, step)$

Logistic map '$(R \times X \times (1 - X))$' will be assigned the value of R that may be from zero to four. The value zero and one are considered separately. However, two will

always generate a value under 0.5, which leads to the right, as opposed to the left, in which the validator has a normal path. The value of three will generate a value under 0.6, which leads the expectation to go right more than it goes left. However, the value of four will generate chaos based on the initial condition. At lines 4 and 15, the R-value will have incremental growth on each step relevant to the depth. The switch from 5–12 is to assess the value of R and act upon it.

4.10 Users community

Humans have many appreciated sins such as forgetting, and unappreciated ones such as unconsciousness; however, society has survived through solidarity, and this has been the basic engine of society, allowing it to flourish as a civilisation, one in which a deterrent for any harmful behaviour of one entity is to inform other entities of a change or to not cooperate, based on evidence which has led to the rest of the belief being harmful. The leaves of the tree contain validators attached to its client communities; sometimes a member will act in ways that are harmful to their environment and, at other times, to validators. One way to deter this behaviour is to inform their community, in addition to other validators in their world. Algorithm 7 describes the process of reputation destruction.

Algorithm 7 Reach community

Input: $User, validator$
Output: $tree$
1 $RequestJustification(Validator)$
2 **if** $this.ID\ is\ User$ **then**
3 Choose once a one from the sequence: $updaterank()$, $removefrominbound()$, or $unsubscribeasaclient()$
4 $informCommunityValidators()$
5 $informCommunityValidators()$
6 $InformUsersInCommunity()$
7 $CallsurfMissa(validator, R)$
8 $node \leftarrow HigherTrustedValidators(concepts, team)$
9 Go Back To *Call surfMissa with high R*
10 Stoping condition is exausting the options or receive a success
11 **if** $this.ID\ is\ validator$ **then**
12 $InformValidators()$
13 $informUserCommunities()$
14 $DynamicallyCouple(user)$
15 Set rule if justification is provided rank is updated positively for validator and negatively for the source

4.11 Dynamic layers coupling

The coupling between the two communities within graph theory has always been a high element of discussion within biological studies due to the importance to interlink between different biological worlds. However, within the police sector coupling has been used to interlink between the polices officers and the dangerous locations. The distributed world has many officers called validators, miners, or maintainers that do

not suffer only from malicious behaviour of the clients that aim to stock the new information but as well from their peers of the same service. Consequently, the dynamic criteria within the graph coupling are very important criteria to maintain the environment because there is a need to jump to another community aiming to secure a fast finality of transaction due to the high level of malicious clients. The other case is to attract clients of malicious validators to join a safe client directory. Following in Algorithm 8 is a representation of a mechanism.

Algorithm 8 Reach community

Input: $Transaction$
Output: $ValidatorProfile$
1 $CommunityStructureliste \leftarrow surfMissa(node, Validator, validatorNumbers, Transaction.receiver, depth, 0, 0)$
2 $validatorProfile.communities.put(size, liste)$

5 Evaluation

5.1 Security discussion

The financial incentive is the driver of miners within blockchain technology. Paxos (Lamport, 2001) and Raft (Clow and Jiang, 2017) favoured fault tolerance and safety to eventually secure a single state of the ledger, whereas Bitcoin favoured liveliness and safety to secure to each node its copy of the ledger. Missa switches the financial motivation from a tragedy of the common to a user's satisfaction to be the centre of interest for maintainers. It preserved all previous advantages, but validators should not be anonymous so they can be incorporated into the taxation system. In the case of anonymity, integrity is secured solely through the intersection's complexity. The approach is based on reputation besides open participation, which eliminates means of monopolisation that leads, eventually, to manipulation. Moreover, anonymity with financial motivation based on a tragedy of the commons was the cause of skepticism due to the inability to punish in the case of a scam.

Figure 4(a) demonstrates the difference in data maintenance between PoW above and Missa down. PoW is simply continuous competitiveness among different anonymous pools not interested in the safety of the user data, but seeking gain from a unique ledger. Each one of the pools is in a race to force its version to achieve financial self-interests. However, Missa approach focuses on the user as a centre of interest as a client. Worldwide adoption with business registered validators will increase trust in the system through huge intersection complexity, besides police support against cyber-attacks coming from the tax benefits.

Malkhi et al. (2019) introduced the concept of corrupt but alive (CBA), in which an adaptive quorum is a solution to maintain validity. CBA can take place conceptually in many other approaches, such as long-range attacks within PoS, leader targeting in improvised Bitcoin-NG (Yin et al., 2018a), or the intention to fork within PoW. Missa invests in the intention of validators to nest a client's directory. It will accelerate block propagation within the network and the validation time, unlike in previous works in a permissionless network. It is not a race to generate the longest sequence of hashes but an intersection of interests with validators that look at any newly generated block as

updated information upon which a probable transaction may be based. Moreover, it is an increase of trust, not just compared to other peers, but compared to the government itself. The interaction for a peer is based on concepts generated from the Rank Function in Algorithm 4 to have a direct connection with territories of interest.

Figure 4 Missa vs. Bitcoin PoW (modularity and deterrence), (a) modularity of data distribution (b) deterrence at the physical level (see online version for colours)

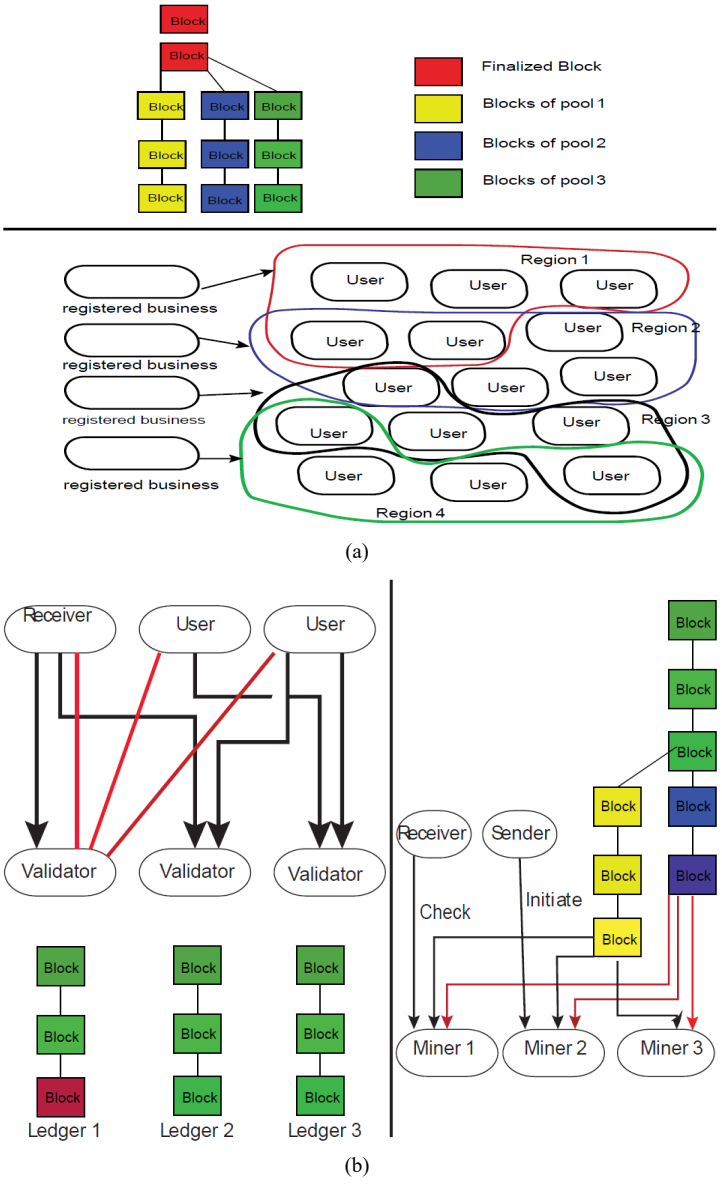


Figure 4(b) demonstrates the difference between the two approaches in terms of finality besides deterrence, in which the finality of the Bitcoin approach is probabilistically

relevant to the number of competing nodes needed to force one ledger, which makes scalability in terms of miners positively correlated with latency. Moreover, post-deterrence is not considered. Missa just aggregates data received from close validators in a certain order, motivated by probabilistic financial motive, and deterrence is maintained through an intersection before reputation destruction that will be applied by the transaction initiator.

The blockchain's transaction receiver may suffer from a double-spend initiated from the sender by using bribery (Liao and Katz, 2017), or by being eclipsed by a monopolising group. Conceptually, the problem lies in the incentive that encourages miners to search for rewards and not reputation. A DoS attack may be used to undermine the network and force double-spend. Thus, probabilistic finality has always been the most interesting concept in the system. The conceptual choice in this problem is the lack of trust with an anonymous entity capable of manipulation, especially in the case of many validators with the same time of block generation. Missa initiates a transaction from the receiver side by getting signed coins, leading the validator to be associated with the receiver for profit. Moreover, the deterrence of validators functions through the chaotic behaviour of Missa to ensure reputation destruction with close communities and the involvement of other competing validators.

A Bitcoin network allows eight outbound and 125 inbound connections by default. Many researchers have investigated approaches to explore the topology to model finality time (Nerurkar et al., 2021). A neighbor discovery service is limited to extracting DNS seeds that represent an ensemble of miners. However, the ability to reconstruct the network virtually raises many concerns as it paves the road to many malicious activities such as RBG hijack, DoS attack, and eclipsing. The integrity within PoW consensus comes from the low pace of injection besides the distribution; however, without the centralising MemPool, the finality latency will increase dramatically. Missa allows a huge distribution as well, but the belief in the node is relevant to the rank, which puts the reputation to be a manager of connections. The validators' topology will be public, but as it is registered as a business, considerations of security measures will be practical enough.

5.2 Environment modelisation

A weak evaluation of the operating environment is provided in this section. The only purpose of this section is to provide a broader view for the reader to observe the proposed system from many sides. Probability theory is the art of describing the subjective interpretation needed to be applied to decision theory to generate action. In all theories there are logical rules, and it is very important to clarify the difference between valid and right. Valid is a possible deduction based on the stated rules that have defined the set of propositions, whereas the right is the consideration of all aspects that define the real world. Following these leads to the valid being equivalent to the right. This section will start by modelling the blockchain environment and, more precisely, the world created by TheTree, in which the following sentence summarises the functioning of the system: "integrity in the system is fostered by the majority of users satisfaction or the low level of malicious activities exhibited in it."

The space of validators is defined as complete, finite, and relationally atomic: X stands for a set of validators. S stands for a system, and Y stands for a set of users.

$$\exists s \in S, \forall x_i, x_j \in X, validator(x_i) \wedge validator(x_j) \\ \rightarrow independence(x_i, x_j, s)(i \neq j) \tag{1}$$

Transforming the foundational sentence stated above to a rule, the assumption within blockchain technology is that user satisfaction is described in terms of the finality of its transaction, whereas malicious activities are described in terms of trust in the validators.

$$\exists s \in S, \forall x \in X, y \in Y \text{ where } X, Y \subset S, Trust(x) \vee finality(y) \\ \rightarrow Itegrity(S) \tag{2}$$

where $Trust(x) \wedge finality(y) = \emptyset$.

The concept of finality within blockchain technology depends on two intersecting concepts, which are the propagation of the transaction to validators and the integrity of the validators themselves, which means their honesty from the user's point of view. T stands for a set of transactions.

$$\forall x \in X, y \in Y, t \in T, propagateTransaction(x, t, y) \wedge honest(x, t) \\ \rightarrow finality(y) \tag{3}$$

The concept of trust in the validators within the blockchain technology, and especially from Missa perspective, depends on two intersecting concepts as well, which are the propagation of the block that contains the transaction and the reputation of the validators. B stands for a set of blocks.

$$\forall x_i, x_j \in X, y \in Y, b \in B, probagateBlock(x, b, y) \wedge reputation(x_i, x_j) \\ \rightarrow Trust(x)(i \neq j) \tag{4}$$

The regularity in probability is a rule which sets a background that all probabilistic propositional assumptions cannot be zero. Thus, each concept must be modelled probabilistically to define the background of the evaluation, in which the constant must manage the growth but must always assume the existence of dissatisfaction'and some malicious activities.

Based on the rule of general additivity applied in equation (2):

$$P(integrity) = P(Trust) + P(finality) \tag{5}$$

Based on the rule of multiplication applied in equations (3) and (4):

$$P(finality) = P(honest) \times P(probagateTransaction \mid honest) \tag{6}$$

$$P(Trust) = P(reputation) \times P(probagateBlock \mid reputation) \tag{7}$$

However, due to the philosophical argument of context applicability, the solution will just consider rules (6) and (7) to be a simple multiplication to secure the evaluation of the impact. The next step is to define low-level concepts such as honesty, the propagation of transactions, the propagation of blocks, and intersection.

$$probagateBlock(b) = \frac{\frac{(\gamma \times size(b))}{MaxSize} + \frac{\delta \times intersection(i)}{regionsNumber} + \frac{\zeta \times power(i)}{MAXPOWER} - \frac{milicious(i)}{AllMilicious}}{3} \tag{8}$$

$$probagateBlock(b) = \frac{\frac{(\delta \times intersection(i))}{regionsNumber} + B_i \frac{\beta \times NumberOfclient(i)}{NumberOfUsers} + \frac{\varsigma \times Conscience(i)}{clientData(i)} - \frac{milicious(i)}{AllMilicious}}{3} \tag{9}$$

$$honest(i) = \frac{(\beta \times intersection)}{NumberOfValidator - \xi \times Risk(i)} \tag{10}$$

$$ProbagateTransaction = 1 - F^{receiversNumbers} \tag{11}$$

First, the centre of the study will be based on a rule (2), the aim of which is to observe continually with an independence each event and how the environment grows and maintains the community t to draw the boundaries of the system management. Second, the study will try to model and evaluate the real-life finality with growing and cumulative user belief toward the system by considering its factor within a delta time, in which rule (2) will be transformed to:

$$\begin{aligned} &\exists s \in S, \forall x \in X, y \in Y where X, Y \subset S, Trust(x) \wedge finality(y) \\ &\rightarrow Integrity(S) \\ &Consequently: \ P(Integrity) = P(Trust) \times P(Finality) \end{aligned} \tag{12}$$

Rule (12) is deduced based on the same comment stated above regarding rules (6) and (7). Rules (8)–(11) have been concluded from the defined data structure of each profile, in which the validator profile that will be followed by his peers is based on the level of intersection, conscience, previous malicious activities, and the power of the used devices. Rule (8) defines the block propagation, which is normalised over three, besides defining the most important components required to secure fast propagation. The speed of the block propagation is based on the size of the block, the level of intersection within the system normalised over the number of regions, and the power before deducting the malicious activities that have happened in the system. Rule (9) will again evaluate reputation based on the intersection level depending on whether the peers are registered as a business or not, before adding two intersection concepts, which are the portion of the clients from the system multiplied by conscience and finality, deducting again the level of malicious activities. Rule (10) will evaluate the honesty of the validator from the user's perspective, in which the level of intersection is the important criterion before deducting the level of risk. Finally, rule (11) evaluates the propagation transaction in terms of the probability of dropping a packet.

Figure 5 shows the growth of parameters against rule (2) with a highly independent event, which dictates the normal growth of the system over the long-term. User parameters over trust in validators does not have the greatest impact on integrity. The fluctuation represents the random choice on the registered companies. This implies that in the long-term, the system is not responsible for the satisfaction of each user but for ensuring a high level of finality. Thus, we can conclude that the system like any other institution is preserved as a global commutative stability built in a growing community that generates finality. A created object named region that contains methods such as immigrate, update parameter and chaos is set. It is embedded in a community object. a list of communities will provide an example of the system. All variables were set to 0.99. All management constants were initially set to 0.01. Special variables such

as risk and malicious are set to 0.1. The constants will be incremented slowly to the norm. From system point view, the figure is just a demonstration of how the variables that correspond to the structure of the network, which has been selected or imposed on TheChain, do not conflict.

Table 1 The definitions of the constants

Constant	*Role*
ς, ζ, δ, ξ, β	Constant to manage the concept presented in the whole platform
MaxSize	The maximum size permitted for a block
regionsNumber	Number of regions to apply normality over intersections
MAXPOWER	Max power to apply normality
AllMilicious	All malicious behaviour in the system
NumberOfUsers	Number of users in the system
clientData	Get the number of submitted client data for validator i
receiversNumebrs	Number of peers to broadcast to
F	Setting the number of losses in the platform
B_i	Business or not (1 or 0)

Figure 5 Non-chaotic experiment with linear growth of parameters, the growth of all parameters defined simultaneously shows more resilience to the platform (see online version for colours)

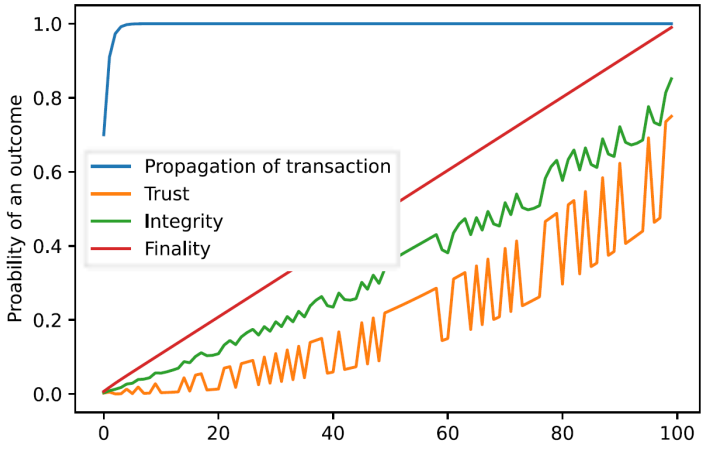
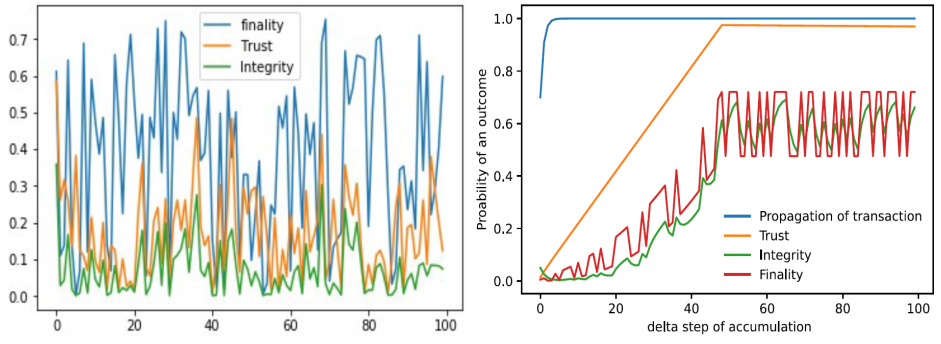


Figure 6 illustrates rule (12), where the intersection case follow delta time but is more focused on the long-term stress of the system by questioning the capacity for chaos. Long-term chaotic behaviour of validators and users will likely reduce system integrity, mainly between 0.0 and 0.1 with the responsible region. The integrity will strongly depend on the continued value of trust and finality due to the commutative emotional feeling expected in case of chaos. Thus, objects were chained which represent the behaviour with the infinity hypothesis on the number of these objects. Immigration is interpreted as higher growth in parameters. Thus, as shown in Figures 6(a) and 6(b), the use of rule (13) resulted in the expected integrity convergence between 0.5 and 0.7

because it strongly depends on confidence in this choice, however, it is Figure 6(a) the chaotic region that drops integrity to 0.1. The demo sequence tries to show how a delta time of chaos does not have a catastrophic impact on the system and to point out that there is a logical separation between the regions which eliminates the expansion of chaos because the trust of the users is associated with the relevant validators. From a system point of view, it is a demonstration of how the emotional effect that leads to the intersection of two concepts will result in a weaker view of integrity for the new community.

Figure 6 (a) Experiment where finality impacts on trust to generate integrity (b) Immigration has resulted in higher growth of parameters that force the conceptual aspect to grow (see online version for colours)



(a) (b)

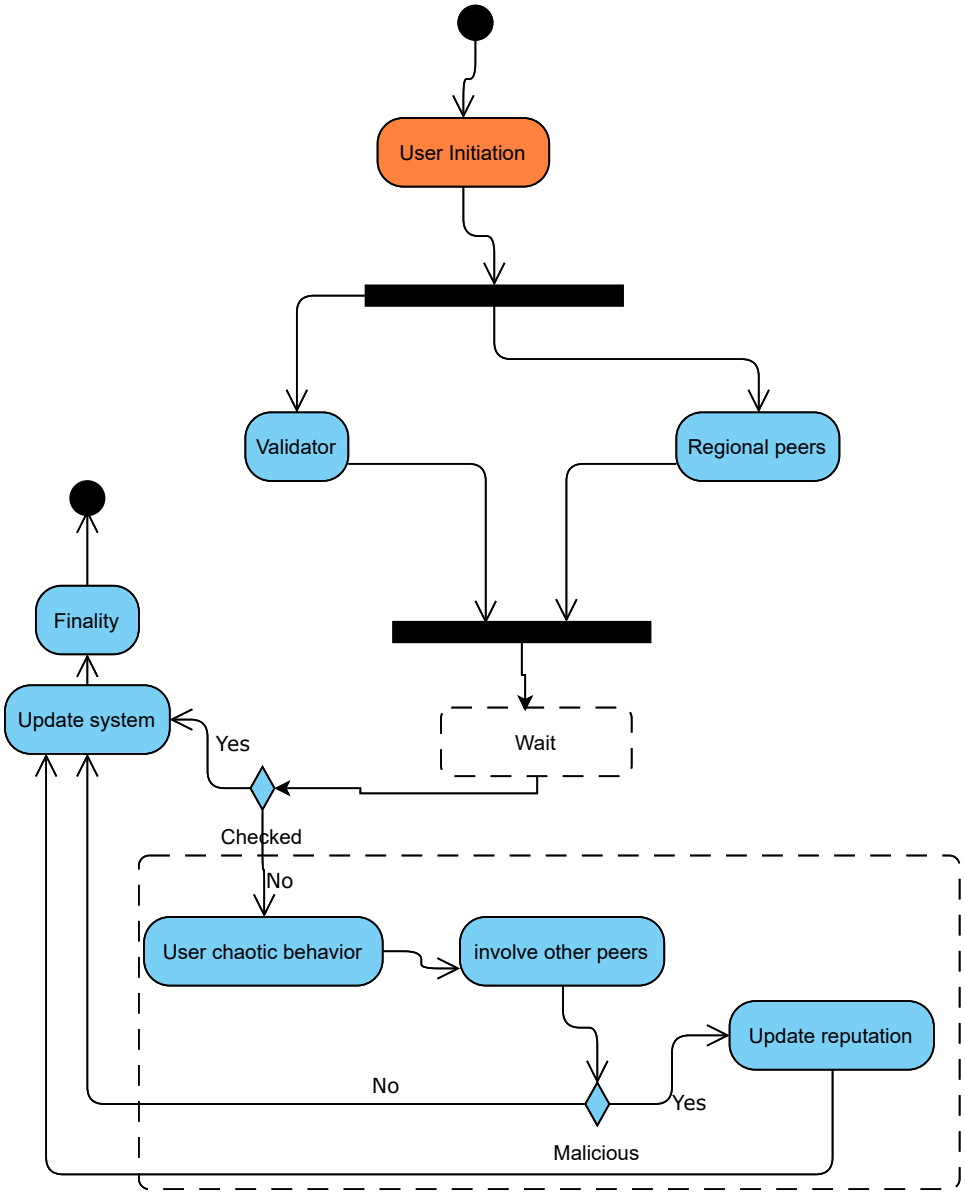
5.3 Formal study

Missa functions over different components to maintain integrity as a final conceptual state. It must be made clear that there are two kinds of peers in the system, building two layers of topology. The user's side, in which a transaction initiator is a receiver, and incentivised by the intention to earn money. Consequently, reputation is very important to attract receivers to be clients. On the other hand, the validator has two kinds of incentives. First, the intention to force consistency with high duplication leading to credible finality. Second is the intention to inform through propagating information. The first criterion is met as a normal cause of the intersection of interests, in which duplication in order is in the financial interest of any validator due to the probability that future transaction fees may be based on it. The second criterion is met by the intention of the validator to finalise the interaction with the user to secure fees.

Figure 7 demonstrates the main activities taken in the validation session. First, the initiation of a transaction from the receiver side is broadcasted to the main validator and his regional peers. Then, awaiting with relevance to a capability of propagation, which is noted in the testing section. Finally, if the trust among validators and their regional peers is low, checking the exterior peers is an option, before inviting them for help in the case of intentional delay. However, the initiator is a receiver, and he holds coins as proof of transfer. If the region delay is intentional and may be associated with double-spending, the reputation will be updated. The states that can be happening in the system are the

following: transaction initiation, user broadcasting, transaction holding (stands for lack of intention to share), peer involvement (assuming there is always someone that helps), updating the system, broadcasting the new state and, in the end, arriving at a transaction finality.

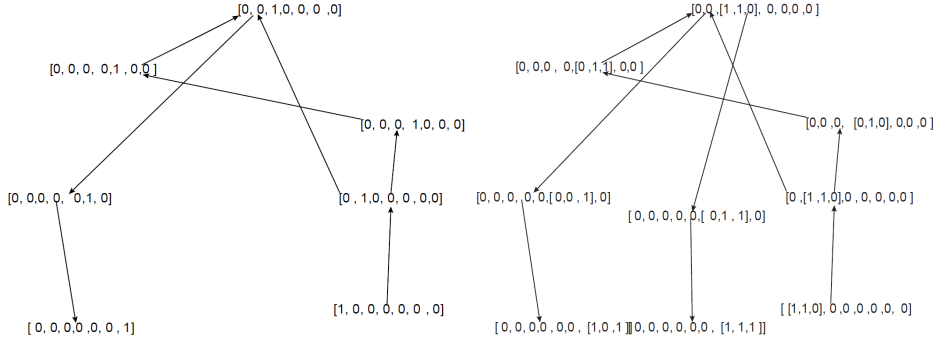
Figure 7 Activity diagram (see online version for colours)



The system always intends to reach finality. The following is a description of the proprieties that are involved in the transition among states. The state transaction initiation has the propositional rule that states: the user is satisfied. User broadcasting

has a rule, which is that the validator is credible, the state transaction holding rule is a user who is not satisfied, and peer involvement means the reputation has been updated. Broadcasting a new rule means the validator is credible, and the finality rule means the user is satisfied. However, the temporal logic between states indicates that, eventually, there will be a finality. The next sequence is derived from the activity diagram. Figure 8 has been generated using the graph reachability algorithm.

Figure 8 Graph reachability



On Figure 8(a), the states are transaction initiation, user broadcasting, system updating, transaction holding, peer involvement, share the new state, and finality. On Figure 8(b), the manipulation of attached proprieties introduced the intern vectors [user satisfaction, validator credibility, reputation updated]. As can be observed, as the assumption has been preserved such as there is always a validator to help with the high complexity of intersection, this will secure, in the end, the user's satisfaction as well as quick finality.

5.4 Comparison

Algorithmic complexity is a way to evaluate the algorithm's expected functioning by evaluating its worst and best execution. The following is a comparison of the system choices before dividing our approach in terms of deciding and dealing with malicious activities.

The decision is a criterion that leads to finality, in which the PoW is a solution based on solving an NP problem by investing huge resources to generate a solution. However, the decision of finality is based on three components, which are the PoW complexity, the broadcasting complexity, and the probability of being the first. On the other hand, PoS inherits randomness, but in a different form, by making a random vote on the next validators before broadcasting, embedded with the probability of submitting a block. Finally, IOTA is based on a small set of NP problems before dealing with the probability of linking transactions above the latter, counting on the high level of submission. However, Missa decision is based on surfing the tree to come to the knowledge of the validator's environment. Thus, the decision is based on the criteria of surfing complexity, broadcasting, and verification.

Table 2 Conceptual choices

	PoW associated technique	*PoS associated technique*	*IOTA approach associated technique*	*Missa associated technique*
Finality type	Probabilistic	Probabilistic	Probabilistic	Deterministic/ probabilistic
Information propagation	Gossiping	Gossiping	Gossiping	Broadcast among committee
Broadcasting complexity	$O(nlog(n))$	$O(nlog(n))$	$O(nlog(n))$	$O(n)$

Table 2 demonstrates the information propagation choices within different proposals, in which IOTA, PoS or PoW platforms use a gossiping algorithm with complexity $(nlog(n))$. The tragedy of the commons incentive over the gossiping protocol leads to hard probabilistic finality. However, Missa on the validators level uses broadcasting within the committee that has been generated through ranking. Therefore, it will be relevant to n in terms of complexity. Missa finality can shift from probabilistic to deterministic with the relevant chaotic value of surfing it.

The only real competitor concept will be the PoW as other approaches fail conceptually to respond to many security criteria. The worst-case form that Missa can take is to be the same as a decreasing recursive function. Consequently, it will have the following representation:

$$f(x) = \begin{cases} node, v \leq worldSize \\ T(v-1), v \geq worldSize \end{cases} \quad \{\text{it will lead the complexity to be } O(v)\}$$

In which v stands for validator list size, worldSize is the limit that each conceptual world must contain on the low level, and a node is a data structure that contains all the saved knowledge about the validator and its environment.

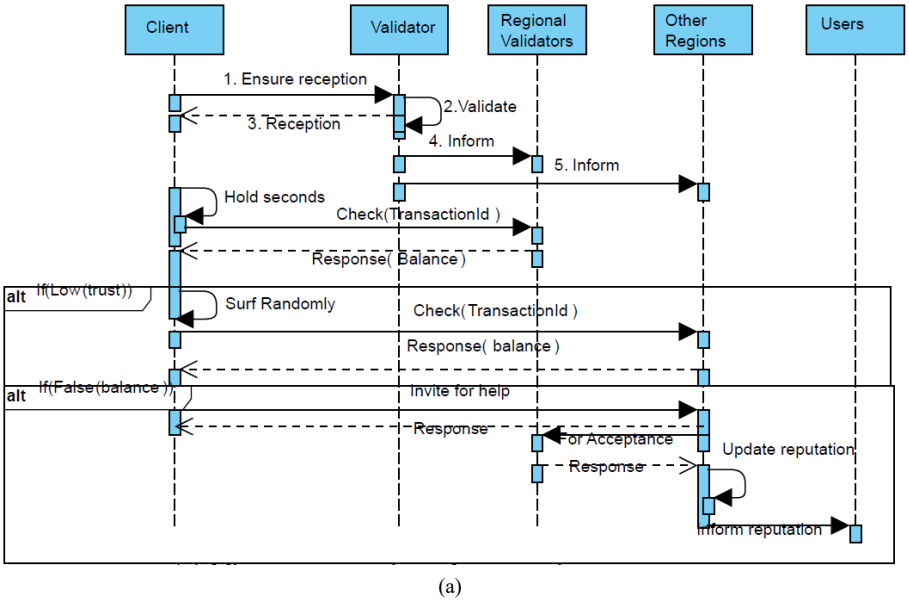
The best-case scenario is when Missa is well balanced, which leads the surfing to be smooth. The following is the representation:

$$f(x) = \begin{cases} node, v \leq worldSize \\ T(\frac{v}{2}) + v, v \geq worldSize \end{cases} \quad \{\text{it will lead the complexity to be } (v^2)\}$$

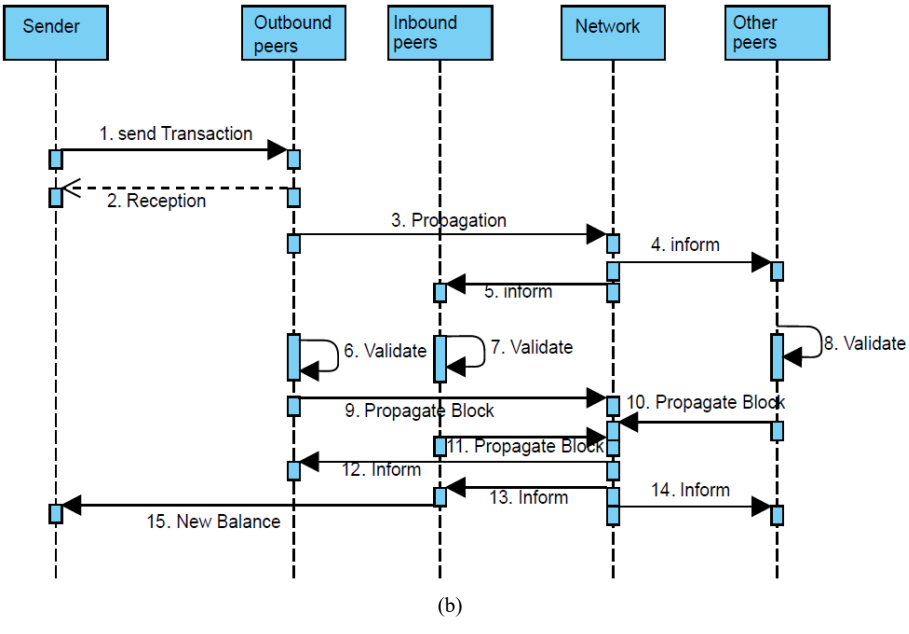
In leaderless blockchain approaches, all validators perform puzzle-solving, useful work, or random sleep. Thus, the solution can be described in $\exists L,\ b,\ c \in B,\ \forall v \in V$, $finality(L) = choose(generate(c, v, b), 1)$ in which v, b, c, and L represent validators, block, processing capacity (Transaction per second), and ledger respectively, and choose will select a single version of a block from all the blocks generated from different related validators with relevance to their capacity. Thus, the level of processing of the transaction in a linear order can be described in $Traitement(t) = \frac{size(t)}{(sizeofblock)} \times Delay$. T represents a list of transactions and delay is the expected delayer for each block separately. However, in leader-based approaches, pipelining and spinning are different options. Pipelining can be described as $\exists v \in V,\ L,\ b \in B,\ finality(L) = generate(c, v, b)$ where one validator is the block generator at a time. Thus, subjecting it to the capacity of a single validator described in $Traitement(t) = \frac{(size(t))}{C}$. However, the spinning increases the capacity (c) in the linear atomic order of processing, as

the pipelining is subject to leader bottlenecks. Finally, Missa allows generation from all validators at the same time with relevance for their client directory. Therefore, transforming it into $\forall v \in V,\ L,\ b \in B,\ finality(L) = generate(c, v, b)$. Will make the traitement processs to be $Traitement(t) = \frac{(t)}{(C \times numberofvalidator)}$. However, Missa worst topology structure performs the same as pipelining.

Figure 9 Sequence diagram, (a) Missa propagation of transactions (b) normal propagation of transactions in the blockchain technology (see online version for colours)



(a)



(b)

Figure 9(a) demonstrates how the sequence of actions with Missa approach is based on the receiver's persistence until the transaction has been injected. The other users serve as social punishment for the non-cooperative nodes. It starts with the receiver's intention to secure the fund, followed by different instructions for checking the system. Finally, it checks the trust in the regional validators before involving other regions until it makes sure the transaction has been injected with success. In the case of malicious behaviour, the social punishment will be there through the reputation being updated. On the other hand, on Figure 9(b), the transaction depends on the initiator, who propagates the transaction using a gossip algorithm that ensures its injection due to the expected zero collaboration in the case of a well-propagated transaction. It starts by sending the transaction to the outbound nodes that will be propagated in the network, which makes sure that all the nodes are aware of it. The different nodes compete over the block, then, with probabilistic finality, the turn will reach the transaction for it to be eventually validated. The receiver, as well as the sender, will be waiting for the upcoming news from their inbound peers. The choice among inbound is random with consideration of their reputation.

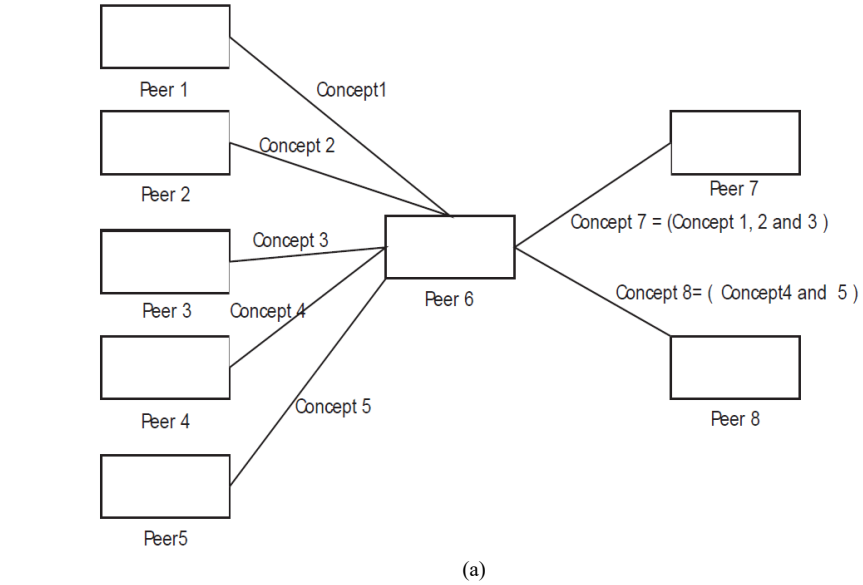
5.5 Conceptual comparison

Blockchain code is not well documented due to the high scale of adoption, which leads to different implementations. However, its architecture has been the focus of academic interest. Many studies have described the network topology, peer modularity, and implementation efficiency. The solution suffers from a software engineering perspective of an unmet legal requirement, low capability of testing due to its distributed nature, medium agility due to standards that have to be met for each peer to run within the environment, low ease of development due to its distributed nature that requires many network considerations and trade-offs, its scalability, coupled with performance, is subject to an eventually probabilistic consistency that defines the system as having low scalability, and it has low network performance concerning convergence. Thus, the concept of reliability is an important criterion, along with the short response latency, scalability, and modularity. Moreover, the solution must address market restrictions, such as legal compliance, a set of standards, and the high cost of its implementation.

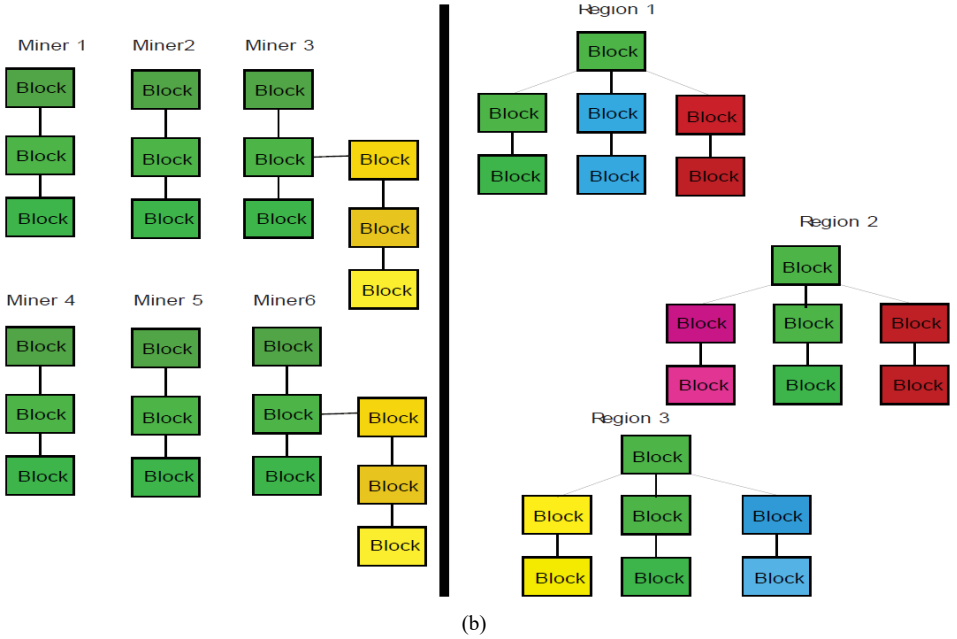
Blockchain technology was dedicated in its first decade to the production of cryptocurrency and, due to its wide adoption, it has also been considered within the insurance sector, finance and government. However, modularity that ensures the agility of the architecture must be met to generate a system that can be easily adopted. It has been observed that systems such as Bitcoin, Ethereum and other implementations that possess a high coupling between the different components have low agility. Missa has proposed the use of a new pattern to model the world into virtual computing components. The solution innovated away from the peer-to-peer pattern or event-oriented design but has built upon it to generate concept management between the two virtual peers on the distribution level of the concept-built regions, which can be an ensemble of concepts of the same type from different peers or different types of concepts. Figure 10(a) demonstrates the pattern which will allow flexible, controllable agility and maintainability of the system on the distributed level. A region of different concepts can be managed as a unique concept. The differentiation of this approach from the modelisation of component-oriented programming frameworks such as OSGi, Corba and fractals is that security issues are related to the concept of a contract that focuses on

the data structure and not information, as well as the middleware implementation that manages the service registration.

Figure 10 Conceptual comparison, (a) concept model (b) eventual consitency (see online version for colours)



(a)



(b)

Reliance in blockchain technology is described as the capability of the system to serve at any time. However, the system's worldwide adoption with its financial gain is subject to horizontal and vertical scalability to ensure reliance. The scalability of the treatment

of the transaction is subject to the CAP theory: in other words, consistency, availability, and partial tolerance. The legal requirement of business registration will allow different validator nodes to legalise their business in the system, as well as ensure a low level of malicious activity that eliminates an eclipsing or RBG hijacking, guaranteeing the concept of partial tolerance. The choice between strong availability and strong consistency has always led to strong availability and weak consistency within a delta time, before eventually achieving consistency. Figure 10(b) demonstrates the difference between Missa and the Bitcoin approach, in which Missa is expected to reach eventual consistency more quickly due to the lack of probabilistic finality related to competence over one version of each block but it is limited to the state of acknowledgment.

Scalability must deal with malicious behaviour in the system. PoW, PoS, Tangle IOTA or BFT are all techniques that use either voting, resources or stakes to force the longest chain or path. However, the monopoly must take place following the longest chain rule. The concept that initiated the blockchain technology was PoW, which used complexity and randomness to deter malicious activities. However, a true elimination of the trusted party must take down the capability to monopolise the system. Missa has taken a different approach, betting on the validity within a high intersection of interest among the different nodes. The following is the expected probability of maintaining a low consensus between nodes. $f = 1 - c^{(n(n-1)/2)}$. If the probability of the coming consensus between the two parties is: $c = 0.99$ it models the probability of coming to a consensus (c) to force a certain state with the ability to bring all other nodes onto the table in a deal that can be modelled with a complete graph. Thus, the probability of not coming into f is what remains of the space minus what is believed to be a consensus. The growth of the number of nodes n will diminish any deals due to exterior factors, such as legal compliance. Finally, the discussed concept provides a good background for setting standards of communication, which will later be the background for legal compliance. The capability to model the world through concepts will allow the easy integration of any component into the system.

6 Testing

The engine of economic growth is the connection between the human delusional evaluation of certain objects and his efforts. Guaranteeing the ownership of the object requires recognition, the finalisation of the exchange and the securing of authenticity. On the distributed information, it can be translated into propagation, final consistency and deterrence of the system. This section is divided into three stages. First, the topological level addresses the impact of platform choices on its functioning by improving its expected propagation time. Second, the consistency level assesses the expected time of the exchange in a manner comparable to the growth of information generation. Third, the safety assessment relies on the convergence of actors in the event of chaotic behaviour.

The blockchain's deterrence against double-spending is achieved by ensuring consistent duplication between many validators. For PoW, there is a delay until a winner is declared in a race leading others to adopt the version and start the same process over again. However, for technical reasons, users will be satisfied after a few more appendages in the ledger. Also, in other approaches such as PoS or BFT proposals, the finality is decided by the global attachment of the transaction. Thus, the techniques associated with the propagation of information followed by the logic ensuring an overall

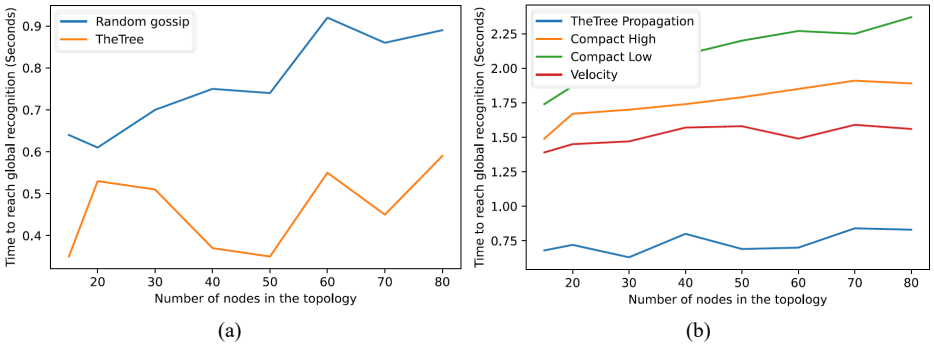
consistent finality are very important in time for comparing the operations of the platform from a user perspective. On the security, the high level of duplication and anonymity associated with PoW has led miners to continue racing as any intentional modification of previously processed information is very costly. On the other hand, BFT and PoS use severe penalties for deterrence. Thus, the evaluation of the cost of malicious behaviour on the operation of the platform is an important factor.

The device used was a Windows 10 Intel 64-bit core i5 machine with a frequency of 1.8 GHz and 8 GB of RAM. NS3 simulation was implemented, 5% packet loss, data rate and delay were real for peers distributed virtually on six continents. Each link was managed with a socket. The block size was 1 MB to 25 MB and the transaction size was 1.2 to 2 KB. Additionally, the actor model implementation was used to simulate the distributed behaviour of the runtime using the AKKA library in Java with Intellij as a development environment. Additional delays have been added to mimic an international execution. On safety, the actors are nested with a decision function and learn from the environment to act in a manner consistent with the protocol because of the high rate of deterrence. This shows that eliminating their cooperation will cause them to harm each other for financial gain and eventually force everyone to obey the law.

6.1 Topological level

Transaction propagation is the first element that takes advantage of the topology to inform all peers of the new knowledge that has been generated. Random gossip is the dominant approach for the propagation of transactions. Thus, it was evaluated in comparison to the Missa approach. On the other hand, block propagation is the second data structure to be exchanged between maintainers. Therefore, the test has demonstrated of Missa and its comparison with the available solutions, such as high, low bandwidth compact block propagation, and velocity. Nodes are highly linked, in which each member has a unique collection of eight peers. Time estimated based on an increasing number of nodes and blocks varying between 1 MB and 25 MB.

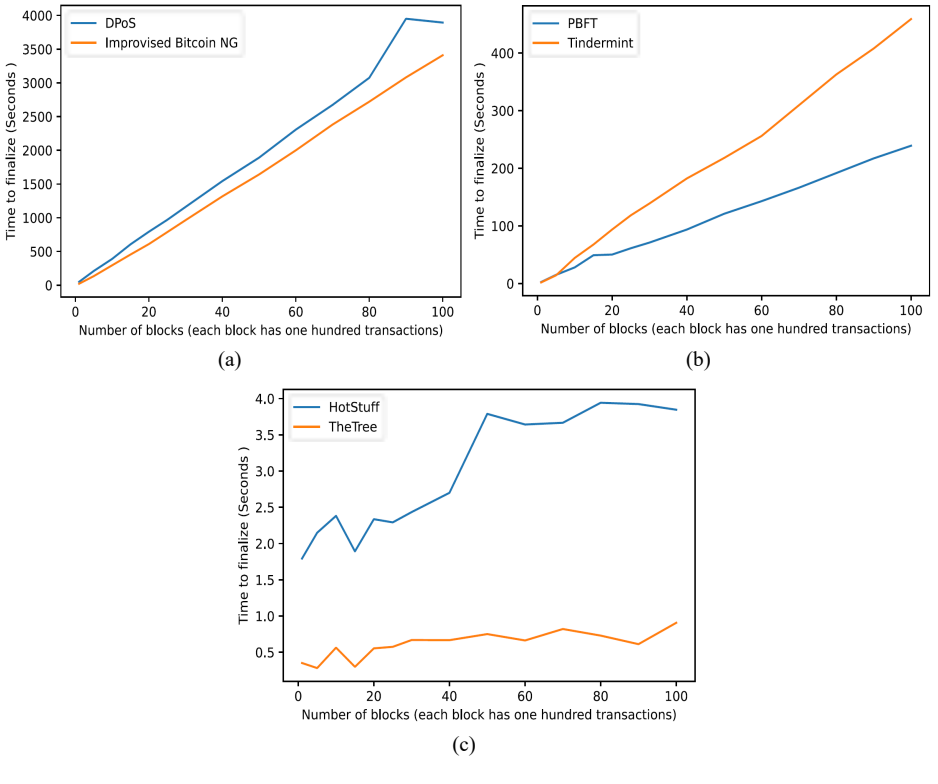
Figure 11 Propagation time, (a) increasing number of nodes within highly coupled topology to demonstrate the expected linear growth to reach global recognition of a transaction (b) increasing number of nodes within highly coupled topology to demonstrate the expected linear growth to reach global recognition of a block (see online version for colours)



(a) (b)

On Figure 11(a), random transaction gossip performs poorly against scaling due to the growth of duplication, but Missa uses source routing to broadcast the transaction to other peers for the pre-verification. In addition, regarding block propagation, Missa's performance is due to a direct link between the interested parties and a geographical consideration at the topological level compared to other approaches which use a random flat topology to offer a vision of anonymity next to the level of exchange. As previously stated, Missa first submits the transaction for pre-verification, then upon receipt of the signed commit, it will submit a block containing the transactions previously pre-verified using source routing. This allows the system to take advantage of the high performance expected of the topology. In addition, scaling will not be a problem as consistency is seen regionally rather than globally. Eliminating double-spending requires rapid dissemination of information. Missa's architectural choices make it the most efficient approach to meet user expectations due to very low linear growth for time propagation in the case of a higher number of nodes and blocks.

Figure 12 Finality and deterrence, (a) the increasing number of blocks in DPoS and improvised Bitcoin-NG compared to the time required to finalise the logic to ensure consistency (b) the increasing number of blocks in Tindermint and PBFT compared to the time required to finalise the logic to ensure consistency (c) the increasing number of blocks in HotStuff and TheTree compared to the time required to finalise the logic to ensure consistency (see online version for colours)



6.2 Consistency level

The logic to be achieved before declaring finality results in a delay for the retrieval of proof of submission, which leads to manipulation of many layers such as leader attack, RBG hijacking, or DOS attack during one of the required steps. However, adding transactions to the general ledger of all peers requires an order. Entering into a world order dictates reaching the finality. BFT approaches, which use an authorised environment, hence the PBFT pipeline, and spinning or a combination of the two approaches have been used as different conceptual solutions to increase throughput with impact on finality. Moreover, a solution such as DpoS, improvised Bitcoin-NG or Tindermint has linear growth due to the need for one version. However, Missa had to focus on the transaction, not the block order before submitting the order based on an invitation provided by other validators.

Figure 12 is a demonstration of expected runtime performance drawn from many sessions of an actor model trial with a random selection among delay and topologies. Hotstuff's high performance is due to the use of PBFT pipelining within an expected permissioned environment. Tendermint uses spinning and the order uses a combination of PBFT and PoS to reach consensus. The downgraded DpoS (Yang et al., 2019) is the worst after pure PoW due to the use of a lite version of it for the selection process before voting that end of comparison of blocks, but improvised Bitcoin-NG works a little better due to the direct random selection process. The security assumption for execution makes Hotstuff better considering the requirements. Missa performs best overall as deterrence is turned into a network, forcing users to submit authentic transactions and validators to force the acknowledged expected order of it. Therefore, it eliminates the probabilistic finality arriving with the blocking order and eventually makes the consistency subject to acknowledgement. The logic ensures reliability on the user side because the proof of reception is a set of registered businesses signatures. In addition, it is the fastest in terms of requirements to propagate and complete the transaction.

6.3 Unit test

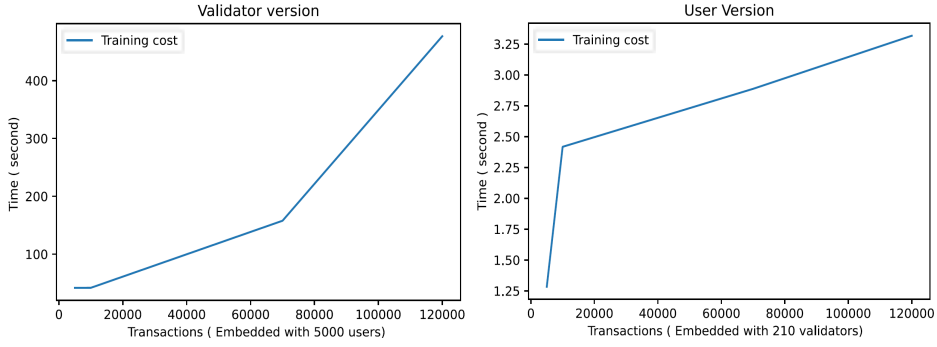
This subsection will present the training and experience required to assess the reputation of management as part of system scale-up. As demonstrated in Figure 13, the growing cost of training in the validator's version is exponential due to the use of a greedy search algorithm for community detection. However, on the fly, detection by dynamic community association will be used, which will be less expensive but, for new validators, the community must be detected through training of Missa. The data used for training is global trade, in which countries represent validators with fake users generated for each transaction.

System of an actor model that has 210 validators and more than 2,000 users. The system ease of operation is expected due to the registration of validators as businesses. Therefore, any malicious behaviour is reflected on a state internal security system. However, in this test, the hypothesis is based on the possible realisation by anonymous validators to demonstrate the cost of malicious activities on the validators and to explain that the logic loop explained previously will force each actor to act honestly because there will be a high rate of deterrence.

Each actor is implemented to seek its interest by aiming to maximise its gain. A validator has a decision object that chooses to act based on preset likelihood between

malicious and honesty based on the size of lost and gained users. It is injected with ranking network (Chandler, 2017) which has four concepts to maximise the gain. It contains the malicious concept which has two links, one to gain customers and one to lose customers, and both then lead to financial gain. If a validator has not received a request for justification, information about a ranking update, or unsubscription from a client for their withholding of a transaction, they will update the malicious act as a positive behaviour. However, negation will update it negatively. On the user side, any logically incorrect information, whether on the metadata or the data itself, will also result in a user update. However, the focus will be on validators as they are the managers of the validity.

Figure 13 Missa training, (a) exponential increase in learning time as the number of transactions is increased (b) exponential increase in learning time as the number of transaction is increased (see online version for colours)



(a) (b)

Running the same parameter a hundred times with a random choice of users in a fraction of ten seconds to initiate a transaction showed that the cost of malicious activity on validators forced them to act honestly after continually updating the ranking function. The malicious act, which is not followed by environmental action, is considered financial gain. However, before these actions are taken, users ask validators to justify themselves. After a while, the system stabilises as the high deterrence rate coupled with strong peers connection led to the update of the ranking function. Convergence time is eliminated because it was heavily dependent on a different initiation (updating ranking with relevant ones for community members, validators, or topology link).

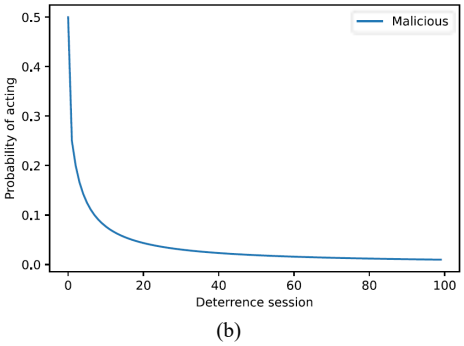
Figure 14(a) shows the actions printed from actor interactions, in which rank update, unsubscribe request, and cut link are different options for customers. However, for validators, the rank update is the main option that prevents the validator from transmitting the signatures of the most malicious validators as proof of recognition to the users, which leads to preventing the extension of their scope of action. Figure 14(b) is generated by manipulating the parameter of several malicious members in each user world. This shows that the level of malicious members within the community, as well as the security provided by validators within a world, is not important as long as there is at least one path to deliver the message to certain users, which led to churns translated deterrent and updated the ranking function. The graph represents many trials with a different set of community solidarity and global security, which represent the number of cooperative users and validators respectively. Stability is achieved when the level of

maliciousness is very low after numerous deterrence stages, in which validators only aim to act honestly. In addition, the updated ranking function quickly escalates but requires a lot of testing to eliminate the maliciousness. The malicious line represents the decreasing actor-level probability of acting maliciously, as it is set to 0.5 and rated with relevance to the gain and number of registered users.

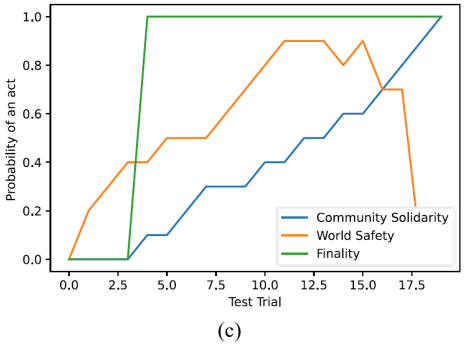
Figure 14 Peers managements, (a) different actions taken in sequence within the deterrence sessions to force the validators to act honestly (b) updating the decision-making function due to financial losses (c) finally comparable to the evolution of the number of malicious activities among users and validators in the same world (see online version for colours)

```
[akka://MainMain/user/$xb] - The validator 95 decided to act maliciously
[akka://MainMain/user/$xb] - The validator 68 decided to act maliciously
[akka://MainMain/user/$pb] - The validator 88 decided to act maliciously
[akka://MainMain/user/$pb] - The validator 79 decided to act maliciously
[akka://MainMain/user/$pb] -  Validator 79has updated rank for user 33
[akka://MainMain/user/$eb] -  Client0Requested to unsubscribe with validator 68
[akka://MainMain/user/$ib] - Client 0 Requested to unsubscribe with validator  72-
[akka://MainMain/user/$fc] - User   150 Requested to unsubscribe with validator 74
[akka://MainMain/user/$6d] -  Client150removed from inbound the validator 79
[akka://MainMain/user/$6d] -  Client150update rank from the validator 79
[akka://MainMain/user/$6d] -  Client150update rank from the validator 53
[akka://MainMain/user/$pb] -  Client150Requested to unsubscribe with validator  79
[akka://MainMain/user/$we ] -Client 178 removed from inbound the validator 89
[akka://MainMain/user/$ye] -  Client 180removed from inbound the validator 88
[akka://MainMain/user/$nb] -  Request justification from77
[akka://MainMain/user/$~d] -  Client 155removed from inbound the validator 63
[akka://MainMain/user/$Fb] -  Request justification from95
[akka://MainMain/user/$Kb] -  Client0 removed from inbound the validator 88
[akka://MainMain/user/$Fb] -  Unjustification provided to clients from validator 95
[akka://MainMain/user/$nb] -  Justification provided to clients from validator77
```

(a)



(b)



(c)

7 Future work

This work has introduced a concept model to respond to modularity, agility and increased scalability in terms of a flexible injection of a new component that manages new kinds of information. Simultaneously, it is recommended as a new approach to

reasoning. Each built world is managed through reputation, and belief is attached to a distributed entity that manages the concept. Moreover, Missa is a data structure distributed in the network to provide knowledge about its structure in terms of a world driven by reputation. The following is a list of directions and the future work that needs to be studied:

1 As the proposal aims to adapt to a user-friendly legal system, the study of the injection of state security representatives into Missa will be studied in a way that preserves user privacy and business transparency.

2 Observing the web in terms of reputable possible worlds can be useful for consistency of information, but the price of isolation is injected. So, it is important to study the user side as a scaling manager, in which users support many validators that handle different heterogeneous/homogeneous concepts will increase competence and mistrust between validators within the business model.

3 Switching decisions from computational components to a network can be followed by considering the user moving from an observation item in simple static terms to a rule generator. The rules will be recorded in different areas of activity, represented in the transaction, to then be explored using algorithms that simulate human behaviours such as kindness, greed or decoding.

4 A node discovery requires the study of the concept of the prior in an open context where a hypothesis on a concept managed by an entity is relevant for the reputation of its world or more. Each node must be seen for a new eye as renowned as its surroundings.

5 Explore more reputation metrics. It can also be a user-generated rule.

6 The approach will be proposed to be implemented at a university to offer students double-blind management and generate tests in real-life scenarios.

7 The creation of an online community for the project and the provision of scenarios that test the correlation between high throughput and security requirements will be provided in a separate work.

8 Conclusions

This work has introduced Missa to provide a structure for approaching validators at the top of a system that increases competence through reputation. A sociological ideology has been injected into the system to deter validators. The concept model is the key to horizontal growth and modularity in the system. The whole system is seen as a new kind of web where consistency relates to the digital world of existence. However, authenticity is a matter of necessity in all worlds. Missa algorithm has been demonstrated, in which reputation is managed through defined criteria with relevance to the community and validator numbers. Moreover, competency at the team division is about choosing a world where validators have less trust in each other. On the associating nodes, it will build a sequence of deterrence by which it will involve finality as the major competitor with high trust. Users will be able to deter users through a random invitation of other validators into the world to execute reputation destruction in case

of a validator's misbehaviour. The approach has been studied in terms of a security discussion, environmental modelisation, a formal study, and a conceptual comparison. Finally, simulation in NS3 and the actor model has been implemented and compared with some models published earlier. The paper can be summarised as follows:

1 discussion of the reputation-based network

2 introduction of Missa algorithm

3 introduction of the concept model

4 theoretical and empirical evaluations have been demonstrated to show the outstanding performance of the proposal.

References

Al-Mashhadi, S. and Manickam, S. (2020) 'A brief review of blockchain-based DNS systems', *International Journal of Internet Technology and Secured Transactions*, Vol. 10, No. 4, pp.420-432.

Awe, K.F., Malik, Y., Zavarsky, P. and Jaafar, F. (2020) 'Validating BGP update using blockchain-based infrastructure', in *Decentralised Internet of Things*, pp.151–165, Springer, Cham.

Belotti, M., Kirati, S. and Secci, S. (2018) 'Bitcoin pool-hopping detection', in *2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*.

Bu, G., Gürcan, Ö. and Potop-Butucaru, M. (2019) 'G-IOTA: fair and confidence aware tangle', in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, April, pp.644–649.

Buchman, E. (2016) *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*, Doctoral dissertation, University of Guelph.

Chan, B.Y. and Shi, E. (2020) 'Streamlet: textbook streamlined blockchains', in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, October, pp.1–11.

Chandler, J. (2017) *Wolfgang Spohn, The Laws of Belief: Ranking Theory and its Philosophical Implications*, Vol. 71, No. 1, 624pp, Dialectica, Oxford University Press, Oxford, ISBN: 9780199697502.

Chawla, N., Behrens, H.W., Tapp, D., Boscovic, D. and Candan, K.S. (2019) 'Velocity: scalability improvements in block propagation through rateless erasure coding', in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, May, pp.447–454.

Chourasia, S. (2013) 'Survey paper on improved methods of ID3 decision tree classification', *International Journal of Scientific and Research Publications*, Vol. 3, No. 12, pp.1–2.

Clow, J. and Jiang, Z. (2017) *A Byzantine Fault Tolerant Raft* [online] https://www.scs.stanford.edu/17au-cs244b/labs/projects/clow_jiang.pdf.

Das, D. (2021) 'Toward next generation of blockchain using improvized Bitcoin-NG', *IEEE Transactions on Computational Social Systems*, Vol. 8, No. 2, pp.512–521.

Delgrande, J.P., Peppas, P. and Woltran, S. (2018) 'General belief revision', *Journal of the ACM*, Vol. 65, No. 5, pp.1–34.

Dotan, M., Pignolet, Y.A., Schmid, S., Tochner, S. and Zohar, A. (2021) 'Survey on blockchain networking: context, state-of-the-art, challenges', *ACM Computing Surveys (CSUR)*, Vol. 54, No. 5, pp.1–34.

Eyal, I. and Sirer, E.G. (2014) 'Majority is not enough: Bitcoin mining is vulnerable', in *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, March, pp.436–454.

Fan, X. and Chai, Q. (2018) 'Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems', in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, November, pp.482–484.

Gladwell, M. (2019) *Talking to Strangers: What We Should Know About the People We Don't Know*, Little, Brown.

Goundar, S., Chand, S., Chandra, J., Bhardwaj, A. and Saber, F. (2021a) 'A taxonomy of blockchain applications', in *Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends*, pp.49–71.

Goundar, S., Shah, Z., Singh, N., Lal, G. and Singh, A. (2021b) 'A literature review in support of blockchain technologies', *Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends*, pp.1–47.

Goundar, S. (2020) *Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends*, World Scientific, Singapore.

Gramoli, V. (2020) 'From blockchain consensus back to Byzantine consensus', *Future Generation Computer Systems*, 1 June, Vol. 107, No. C, pp.760–769.

Haldimann, J., Sauerwald, K., von Berg, M., Kern-Isberner, G. and Beierle, C. (2021) 'Towards a framework of Hansson's descriptor revision for conditionals', in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, March, pp.889–891.

Iacona, A. (2021) *LOGIC: Lecture Notes for Philosophy, Mathematics, and Computer Science*, pp.1–250, Springer.

Kern-Isberner, G., Bock, T., Sauerwald, K. and Beierle, C. (2019) 'Belief change properties of forgetting operations over ranking functions', in *Pacific Rim International Conference on Artificial Intelligence*, Springer, Cham, August, pp.459–472.

Khaldun, I. (2015) *The Muqaddimah: An Introduction to History-Abridged Edition*, Princeton University Press, New Jersey, USA.

Kiayias, A. and Russell, A. (2018) *Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol*, Cryptology ePrint Archive.

Kim, S.K., Ma, Z., Murali, S., Mason, J., Miller, A. and Bailey, M. (2018) 'Measuring ethereum network peers', in *Proceedings of the Internet Measurement Conference 2018*, October, pp.91–104.

Kumar, M.A., Radhesyam, V. and Srinivasarao, B. (2019) 'Front-end IoT application for the Bitcoin based on proof of elapsed time (PoET)', in *2019 Third International Conference on Inventive Systems and Control (ICISC)*, IEEE, January, pp.646–649.

Lai, H.H. (2019) 'How plausible is the relative plausibility theory of proof?', *The International Journal of Evidence and Proof*, Vol. 23, Nos. 1–2, pp.191–197.

Lamport, L. (2001) 'Paxos made simple', *ACM SIGACT News (Distributed Computing Column)*, December, Vol. 32, No. 4/121, pp.51–58.

Liao, K. and Katz, J. (2017) 'Incentivizing blockchain forks via whale transactions', in *International Conference on Financial Cryptography and Data Security*, Springer, Cham, April, pp.264–279.

Loe, A.F. and Quaglia, E.A. (2018) 'Conquering generals: an NP-hard proof of useful work', in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, June, pp.54–59.

Malkhi, D., Nayak, K. and Ren, L. (2019) 'Flexible Byzantine fault tolerance', in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, November, pp.1041–1053.

Mei, W. (2019) 'Formalization of fuzzy control in possibility theory via rule extraction', *IEEE Access*, Vol. 7, pp.90115–90124.

Nacer, M.I., Prakoonwit, S. and Prakash, E. (2021) 'TheCoin: privacy and security considerations within blockchain transactions', in *2021 2nd Asia Service Sciences and Software Engineering Conference*, February, pp.10–17.

Nakamoto, S. and Bitcoin, A. (2008) *A Peer-to-Peer Electronic Cash System*, Vol. 4 [online] https://bitcoin.org/bitcoin.pdf (accessed 15 January 2022).

Nencha, C. (2021) 'Necessitism, contingentism, and Lewisian modal realism', *Acta Analytica*, Vol. 37, pp.1–21.

Nerurkar, P., Patel, D., Busnel, Y., Ludinard, R., Kumari, S. and Khan, M.K. (2021) 'Dissecting Bitcoin blockchain: empirical analysis of Bitcoin network (2009–2020)', *Journal of Network and Computer Applications*, Vol. 177, p.102940.

Ozisik, A.P., Andresen, G., Levine, B.N., Tapp, D., Bissias, G. and Katkuri, S. (2019) 'Graphene: efficient interactive set reconciliation applied to blockchain propagation', in *Proceedings of the ACM Special Interest Group on Data Communication*, pp.303–317.

Prabhu, Y. and Varma, M. (2014) 'FastXML: a fast, accurate and stable tree-classifier for extreme multi-label learning', in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August, pp.263–272.

Recabarren, R. and Carbunar, B. (2017) *Hardening Stratum, The Bitcoin Pool Mining Protocol*, arXiv preprint arXiv:1703.06545.

Rizun, P.R. (2016) 'Subchains: a technique to scale Bitcoin and improve the user experience', *Ledger*, Vol. 1, pp.38–52.

Roy, N., Shen, S., Hassanieh, H. and Choudhury, R.R. (2018) 'Inaudible voice commands: the long-range attack and defense', in *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pp.547–560.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. and Mohaisen, D. (2020) 'Exploring the attack surface of blockchain: a comprehensive survey', *IEEE Communications Surveys and Tutorials*, Vol. 22, No. 3, pp.1977–2008.

Sayeed, S. and Marco-Gisbert, H. (2019) 'Assessing blockchain consensus and security mechanisms against the 51% attack', *Applied Sciences*, Vol. 9, No. 9, p.1788.

Shalini, S. and Santhi, H. (2019) 'A survey on various attacks in Bitcoin and cryptocurrency', in *2019 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, April, pp.220–224.

Silvano, W.F. and Marcelino, R. (2020) 'IoTA tangle: a cryptocurrency to communicate internet-of-things data', *Future Generation Computer Systems*, Vol. 112, pp.307–319.

Singh, D. and Garg, R. (2021) 'NI-Louvain: a novel algorithm to detect overlapping communities with influence analysis', *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 9, pp.7765–7774.

Sohrabi, N. and Tari, Z. (2020) 'ZyConChain: a scalable blockchain for general applications', *IEEE Access*, Vol. 8, pp.158893–158910.

Stathakopoulou, C., David, T. and Vukolic, M. (2019) *MIR-BFT: High-Throughput BFT for Blockchains*, arXiv preprint arXiv:1906.05552.

Tang, S., Zheng, J., Deng, Y. and Cao, Q. (2021) 'Resisting newborn attacks via shared proof-of-space', *Journal of Parallel and Distributed Computing*, Vol. 150, pp.85–95.

Tuzi, D. (2018) *Cryptonight GPU Mining Efficiency*, Master's thesis.

Vyas, C.A. and Lunagaria, M. (2014) 'Security concerns and issues for Bitcoin', *International Journal of Computer Applications*, pp.10–12.

Wang, Z., Liu, J., Zhang, Z., Zhang, Y., Yin, J., Yu, H. and Liu, W. (2019a) 'A combined micro-block chain truncation attack on Bitcoin-NG', in *Australasian Conference on Information Security and Privacy*, Springer, Cham, July, pp.322–339.

Wang, Q., Wang, T., Shen, Z., Jia, Z., Zhao, M. and Shao, Z. (2019b) 'Re-tangle: a reram-based processing-in-memory architecture for transaction-based blockchain', in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, IEEE, November, pp.1–8.

Wu, D., Liu, X.D., Yan, X.B., Peng, R. and Li, G. (2019a) 'Equilibrium analysis of Bitcoin block with holding attack: a generalized model', *Reliability Engineering and System Safety*, Vol. 185, No. C, pp.318–328.

Wu, K., Dai, G., Hu, X., Li, S., Xie, X., Wang, Y. and Xie, Y. (2019b) 'Memory-bound proof-of-work acceleration for blockchain applications', in *Proceedings of the 56th Annual Design Automation Conference*, June, pp.1–6.

Yan, X. and Jia, M. (2018) 'A novel optimized SVM classification algorithm with multi-domain feature and its application to fault diagnosis of rolling bearing', *Neurocomputing*, 3 November, Vol. 313, pp.47–64.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N. and Zhou, M. (2019) 'Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism', *IEEE Access*, Vol. 7, pp.118541–118555.

Yin, J., Wang, C., Zhang, Z. and Liu, J. (2018a) 'Revisiting the incentive mechanism of Bitcoin-NG', in *Australasian Conference on Information Security and Privacy*, Springer, Cham, July, pp.706–719.

Zadeh, L.A. and Aliev, R.A. (2018) *Fuzzy Logic Theory and Applications: Part I and Part II*, World Scientific Publishing, Singapore.

Zamani, M., Movahedi, M. and Raykova, M. (2018) 'RapidChain: scaling blockchain via full sharding', in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, October, pp.931–948.

Zhang, S. and Lee, J.H. (2019) 'Double-spending with a sybil attack in the Bitcoin decentralized network', *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 10, pp.5715–5722.