

Consensus in Blockchain Systems with Low Network Throughput: A Systematic Mapping Study

1st Henrik Knudsen

Department of Computer Science

Norwegian University of Science and Technology Norwegian University of Science and Technology

Trondheim, Norway

henriknu@stud.ntnu.no

2nd Jakob Svennevik Notland

Department of Computer Science

Trondheim, Norway

jakob.notland@ntnu.no

3rd Peter Halland Haro

Sintef Nord AS

Sintef Nord

Tromsø, Norway

peter.haro@sintef.no

4th Truls Bakkejord Ræder

Sintef Nord AS

Sintef Nord

Tromsø, Norway

truls.rader@sintef.no

5th Jingyue Li

Department of Computer Science

Norwegian University of Science and Technology

Trondheim, Norway

jingyue.li@ntnu.no

Abstract—Blockchain technologies originate from cryptocurrencies. Thus, most blockchain technologies assume an environment with a fast and stable network. However, in some blockchain-based systems, e.g., supply chain management (SCM) systems, some Internet of Things (IOT) nodes can only rely on the low-quality network sometimes to achieve consensus. Thus, it is critical to understand the applicability of existing consensus algorithms in such environments. We performed a systematic mapping study to evaluate and compare existing consensus mechanisms' capability to provide integrity and security with varying network properties. Our study identified 25 state-of-the-art consensus algorithms from published and preprint literature. We categorized and compared the consensus algorithms qualitatively based on established performance and integrity metrics and well-known blockchain security issues. Results show that consensus algorithms rely on the synchronous network for correctness cannot provide the expected integrity. Such consensus algorithms may also be vulnerable to distributed-denial-of-service (DDoS) and routing attacks, given limited network throughput. Conversely, asynchronous consensus algorithms, e.g., Honey-BadgerBFT, are deemed more robust against many of these attacks and may provide high integrity in asynchrony events.

Index Terms—Blockchain, consensus, security, integrity, performance and supply chain

I. INTRODUCTION

Blockchain has evolved significantly since its initial roots from Bitcoin and has seen adoption with novel use of the technology for healthcare [1], banking [2], control systems [3], and SCM [4]. In SCM systems, different actors are working together to deliver timely and quality products to their customers. A consensus algorithm used in SCM systems shall provide high transaction throughput to take advantage of vast amounts of IOT sensor data. Furthermore, it would need to function well in an environment with varying network delays. Some nodes, e.g., nodes to collect and transfer temperature data of fresh food on trucks or vessels, may have poor or no internet connection. The blockchain system will be subject to the CAP theorem [5], which is challenging, given high

requirements towards transaction throughput and the constraint caused by an unstable network environment.

This study aims to study to which degree existing consensus algorithms can provide integrity and security with limited network throughput and low network quality. Our primary research hypothesis theorizes that there is little empirical knowledge of blockchain applications' effectiveness with limited network throughput concerning the consensus mechanisms. We performed a mapping study and covered published and preprint articles. Our study aimed at answering the following research questions.

RQ1: How well existing consensus algorithms can provide integrity in an environment with limited network throughput?

RQ2: How well existing consensus algorithms can provide security in an environment with limited network throughput?

We identified and analyzed 25 consensus algorithms qualitatively in this study. The results show that many existing consensus algorithms are unfit for use in an environment affected by varying network throughput. Some consensus algorithms which assume a partially synchronous network can provide integrity in events of asynchrony. However, their transaction throughput may be significantly reduced when faced with targeted denial-of-service attacks. Consensus algorithms that do not make synchronization assumptions, adapted to an asynchronous network, may avoid both.

The remainder of the paper is organized as follows. Section 2 lists related work. Section 3 explains the research design and implementation. Section 4 present the research result. Section 5 discusses the results and Section 6 concludes the study.

II. RELATED WORK

Studies, e.g., [6]–[10], have focused on reviewing the state of the art consensus algorithms. [6] defined a five-component framework for categorizing blockchain consensus algorithms, provided a comprehensive review of current consensus algorithms, and evaluated the algorithms' performance according

to their fault tolerance and throughput. [7] analyzed the algorithm's throughput, mining incentive, decentralization, and security challenges. [10] provided a game-theoretic point of view and looked at the mining incentive provided by different consensus algorithms. Gramoli [8] evaluated the Proof-of-Work (PoW) scheme of cryptocurrencies like Bitcoin and Ethereum according to traditional Byzantine consensus algorithms, and provided insight into PoW specific security challenges, like the Bitcoin anomaly and balancing attacks. [9] provided an extensive mapping of consensus algorithms, according to their architecture and paradigm, and highlighted fundamental differences between public and private blockchain systems, and showed how this impacts the algorithms' applicability in these specific types of systems.

Other studies, e.g., [11], [12], have focused on security challenges related to using blockchain technology. In particular, the studies highlighted the security implications the choice of consensus algorithm has upon the overall blockchain system. [11] provided a comprehensive overview of security and privacy aspects of blockchain technology, defined core security properties, and described existing security techniques. Sayeed and Marco-Gisbert [12] assessed major Nakamoto style consensus algorithms against the 51% attack, as well as other major security threats towards blockchain systems, and reviewed current mitigation techniques.

Both industry and academia have shown great interest in assessing new use cases for blockchain technology, following its success within the cryptocurrency space [13]–[16]. Belotti, Božić, Pujolle, *et al.* [13] provided a *vademecum* to guide designers in their decisions for when and how to apply blockchain technology to their specific use case. Reference [14] presented a systematic review of blockchain within the energy sector and discussed its limitations and potential use cases. Reference [15] reviewed current blockchain initiatives and highlighted domains having real-world technology adoption. Bodkhe, Mehta, Tanwar, *et al.* [16] presented a comprehensive analysis of the state of the art consensus algorithms and their appropriateness related to cyber-physical systems. In particular, the authors outlined domain-specific challenges for supply chain management blockchain systems.

Another exciting research area has been the interconnection of blockchain technology and IOT systems. Several studies, e.g., [17], [18], have been dedicated to describing the state of the art IOT blockchain systems and their challenges. Reference [17] provided an extensive analysis of key components of IOT blockchain systems and promising consensus schemes and reviewed major IOT blockchain projects. [18] reviewed core security issues related to IOT systems and how blockchain technology might be applied to solve some of these issues. The research goals of the related studies mentioned above are summarized in Table I. Furthermore, the consensus algorithms they discussed are summarized in Table II.

None of the related studies highlight the challenge of consensus in environments with varying network delays. In particular, in the context of supply chain management systems, real-world scenarios often involve entities transporting

goods over larger geographical areas, with periods of poor or no internet connection. To deliver on the promises of traceability, accountability, and improved information sharing, SCM blockchain systems' underlying consensus algorithm must allow for efficient data sharing between stakeholders, despite participants being affected by varying network delays. Therefore, assessing the state of the art consensus algorithms' performance under such an environment is essential to find suitable consensus algorithms for SCM blockchain systems. Furthermore, such an analysis may uncover the need for designing novel consensus mechanisms if current mechanisms are found insufficient for the use case.

III. RESEARCH DESIGN AND IMPLEMENTATION

This study aims to provide insight into core mechanisms of the state of the art consensus algorithms and how they relate to SCM blockchain systems in an enterprise setting with multiple stakeholders affected by varying network throughput.

A. Data collection

We followed the systematic mapping study guideline proposed by [19]. The search query "*Blockchain AND Consensus Algorithm*" was used to identify papers related to consensus in blockchain systems. The query was executed at Oria [20], a search engine aggregating research papers from scientific databases, including IEEE Xplore, Springer, ACM Digital library, and Scopus. We included only peer-reviewed research papers in this round of search. Furthermore, to also gain insight into the current non-peer-reviewed literature, the aforementioned search query was also executed towards Arxiv.org. This combined search is meant to provide a holistic view of the current literature on consensus mechanisms applicable to blockchain systems. To exclude irrelevant papers, we first read through the papers' titles and abstracts. Papers that did not explicitly mention consensus algorithms were excluded. Papers that were not available online were also excluded. Furthermore, we excluded any paper that does not provide an adequate description of the algorithm or sufficient security analysis.

A total of 2151 papers were identified via the Oria search engine. Through disregarding non-peer-reviewed papers, the total was narrowed down to 451 papers. We then read through the papers' titles and abstracts to exclude any paper that did not explicitly mention consensus algorithms and got 81 papers. Of these 81 papers, 63 papers were identified as studies that presented consensus algorithms. Regarding the search executed at Arxiv.org, a total of 103 papers were identified. The papers were analyzed in the same manner as with the Oria search. To get representative consensus algorithms, We only include consensus algorithms if they were discussed in more than one paper. We end up with a total of 25 consensus algorithms to analyze.

B. Data analysis

Our classification is based on qualitative analysis and uses a classification scheme differing from [19] because none of the

Reference ID	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]
Review existing consensus algorithms	x	x	x	x	x	x	x	x	x	x	x	x	x
Review and analyze current blockchain projects			x					x	x	x		x	x
Security analysis		x	x			x	x						
Provide analysis framework	x	x											
Present domain specific use cases								x	x	x	x	x	x

TABLE I
RESEARCH GOALS OF RELATED STUDIES

Reference ID	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]
Proof of Work (PoW)	x	x	x	x	x	x	x	x	x	x	x	x	x
Proof of Stake (PoS)	x	x		x	x	x	x	x	x	x	x	x	x
Delegated Proof of Stake (DPOS)	x	x		x		x	x	x	x	x	x		x
Proof of Authority (PoAuth)	x			x		x		x	x	x		x	
Proof of Elapsed Time (PoET)	x	x		x	x	x		x	x		x		
Proof of TEE-Stake (PoTS)	x										x		
Proof of Retrievability (PoR)	x			x	x								
Proof of Weight (PoWeight)		x											
Proof of Burn (PoB)		x		x	x				x	x	x	x	x
Proof of Capacity (PoC)		x		x					x	x	x	x	x
Proof of Importance (PoI)		x		x				x		x	x	x	
Proof of Authority (PoA)		x		x	x				x	x			
Practical Byzantine Fault Tolerance (PBFT)	x	x	x	x		x		x	x	x	x	x	x
Delegated Byzantine Fault Tolerance (Delegated BFT)		x		x							x		
Democratic Byzantine Fault Tolerance (Democratic BFT)			x										
Byzantine Fault Tolerant State Machine Replication (BFT-SMART)				x									
Honey-Badger Byzantine Fault Tolerance (Honey-Badger BFT)	x			x		x							
Ripple Protocol Consensus Algorithm (RPCA)	x		x	x				x		x	x	x	
Stellar Consensus Protocol (SCP)				x				x					
Byzantine Fault Tolerance based Proof of Work (BFT-based POW)					x			x					
Byzantine Fault Tolerance based Proof of Stake (BFT-based POS)	x			x	x	x		x					
Paxos											x		
Raft				x		x		x			x		

TABLE II
CONSENSUS ALGORITHMS IN RELATED STUDIES

identified papers sufficiently covered the topic of consensus in low throughput networks. To classify performance of the consensus algorithms and to answer RQ1, we applied the metrics shown in Table III.

- Reference [21] define read and transaction latency and read and transaction throughput as essential performance metrics. In this study, we are specifically interested in evaluating consensus mechanisms in relation to a blockchain system affected by low network throughput, distributed over a greater geographical area. Thus, the particular focus of the classification is attributed to communication-related costs, in the form of *consensus latency* and *communication complexity*.
- To avoid the impossibility result [22], one can assume that the underlying communication network is synchronous. However, the network may be particular asynchronous

[23] because of the limited network throughput. Thus, the consensus algorithms' *timing assumptions* are also included as a metric. The timing assumptions made by consensus algorithms can be categorized accordingly.

- **Synchronous:** There exist a known fixed upper bound Δ on the message delay between peers within the network.
- **Partial Synchronous:** Either of the following statements holds:
 - i There exists an upper bound Δ on the message delay between peers within the network, but it cannot be known a priori.
 - ii There exists an upper bound Δ on the message delay between peers within the network, but it does not hold before an unknown point of time T .

- **Asynchronous:** There is no known fixed upper bound Δ on the message delay between peers within the network.
- *Byzantine fault tolerance* and *transaction finality* are included, highlighting the algorithms’ resilience towards adversarial attacks, as well as transaction confirmation time. A consensus algorithm’s transaction finality is the algorithm’s guarantee that committed transactions cannot be reversed. Some consensus algorithms providing probabilistic finality, e.g., Nakamoto style consensus, favor availability over strong consistency. Other consensus algorithms providing immediate finality, e.g., BFT style consensus, need strong consistency to enforce this, thus sacrificing the system’s availability during network partitioning.

Metrics	Description
Consensus latency	Number of Round-trip time (RTT) needed to complete a round of consensus.
Communication complexity	Number of messages needed to complete a round of consensus.
Timing assumptions	Timing assumptions made by the consensus model related to the underlying network. This relates to a synchronous, partial synchronous or asynchronous network.
Byzantine Fault Tolerance	The percentage of adversarial control in the network, in which the consensus model can resist double spend attacks.
Finality	The assurance that transactions committed will not be reverted. Either immediate or probabilistic.

TABLE III

METRICS TO MEASURE PERFORMANCE AND TO ANSWER RQ1

To answer RQ2, we first identified core security issues related to the blockchain system based on [11] and [12]. The identified security issues are shown in Table IV. In terms of the SCM setting, with a permissioned blockchain system affected by limited network throughput, not all security issues listed in Table IV are relevant. For example, given that participants in the system are authenticated, a Sybil attack can effectively be combated. In an authenticated setting, aspects like user anonymity and transaction unlinkability are deemed irrelevant. We excluded irrelevant security issues and classified the consensus algorithms based only on double-spend attacks, balance attacks, Long-range attacks, $p + \epsilon$ attacks, DDOS attacks, and BGP attacks.

IV. RESEARCH RESULTS

We first classified the 25 consensus algorithms identified from the literature into five categories, namely, Nakamoto, Byzantine Fault Tolerant (BFT), Federated Byzantine Agreement (FBA), Hybrid, and Crash Tolerant, based on their core principles. Then, we analyzed 1) whether the algorithm provides sufficient performance in this specific application scenario with limited network throughput; 2) whether the algorithms provide integrity in the application scenario, as of RQ1; 3) to what extent the algorithms provides security in this

application scenario, as of RQ2. The findings related to the performance metrics are summarized in Table V. The answers to RQ1 and RQ2 are summarized in Table VI.

A. Performance

Nakamoto style consensus algorithms usually provide consensus in a single communication step, except PoA. They all operate with linear complexity as well as requiring an honest majority. The timing assumption is synchronous, which is challenging with low network throughput. With probabilistic finality, there is also a great chance of forking given our SCM application scenario.

BFT style consensus algorithms usually provide consensus in a three communication step process, with quadratic communication complexity. Delegated BFT, Mixed BFT, and Linear-BFT can achieve linear communication complexity through partitioning the network. Delegated BFT and Mixed BFT delegate consensus to a subset of the nodes in the network. Linear-BFT reduces the number of messages sent per node by using an expander graph. This, however, comes at the cost of either significantly increased centralization or potentially higher consensus latency. BFT style consensus algorithms all provide deterministic finality, which may be of major benefit, providing low confirmation latency for transactions. In the enterprise setting, this can be a deciding factor. These consensus algorithms can typically withstand a maximum of $\frac{1}{3}$ Byzantine nodes, posing a significantly weaker resistance than the honest majority threshold provided by Nakamoto style consensus algorithms. Linear-BFT emerges as a promising innovation, providing the optimal threshold of $\frac{1}{2}$ Byzantine nodes, while also having amortized optimal communication complexity of $\Theta(n)$.

FBA style consensus algorithms do not provide any guarantees to the number of consensus steps involved in agreeing upon a set of transactions. As nodes only communicate within their respective quorum slice, communication complexity depends on each node’s quorum slice’s size. In Ripple, Unique Node Lists (UNL) need to overlap 90% across the network to ensure security, making communication complexity $\Theta(n^2)$. In SCP, nodes are free to pick their quorum slices based on their own reasoning (e.g., reputation, wealth, brand). In an optimistic setting, where the size of quorum slices is constant, SCP’s communication complexity is $\Theta(n)$. SCP furthermore provides optimal resilience towards Byzantine nodes in the federated setting, only requiring that nodes’ quorum slices intersect honestly. RPCA makes an assumption of a maximum of 20% Byzantine nodes for a given UNL list. As FBA agreement builds upon nodes’ quorum slices intersecting, consensus relies on that not all these interconnections are faulty. If these critical nodes suffer from low network throughput, this could hamper the speed and throughput in which the network can process transactions. In particular, if they cannot respond for a long time, transaction throughput may halt.

Hybrid style consensus algorithms typically provide consensus in linear communication complexity using a three-step BFT style process to reach consensus, while using mechanisms

Name	Description
Consistency	Which approach will the system utilize to ensure the consistency of the system's ledger?
Tamper-Resistance	Is the system able to ensure the integrity of the ledger?
Byzantine Fault Tolerance	To which an extent do the system need to tolerate Byzantine faults, e.g. adversarial nodes?
Sybil attack	How will the system protect against malicious actors creating multiple fake identities, attempting to outvote an honest majority?
Double spend attack	How will the system prevent nodes spending the same currency for two separate transactions? Specifically related to cryptocurrency systems.
Long-Range attack	To which extent is the system vulnerable to Long-Range attacks; forking the blockchain at its genesis block and privately building an alternative chain?
P+ Epsilon attack	To which extent is the system vulnerable to P+ Epsilon attacks; taking advantage of the dominant strategy among network participants, leveraging non-altruistic participants against the system?
Balance attack	To which an extent is the system vulnerable to balancing attacks; splitting the network into sub-networks, delaying transactions and performing double spend attacks?
Border Gateways Protocol (BGP) Hijacking	How will the system handle adversarial attacks against the network's routing mechanisms; partitioning the network or delaying block propagation?
Distributed-Denial-of-Service (DDOS) susceptibility	To which an extent is the system susceptible to DDOS attacks, in terms of impact upon safety and liveness? Especially relevant for leader based consensus models.
Degree of centralization	To which an extent is the system centralized around a subset of participants? This may have implications on various double spend attacks, as well as DDOS susceptibility.
User anonymity	Are participants of the system able to partake in transactions while staying anonymous?
Transaction confidentiality	To which extent are transactions kept confidential?
Transaction unlinkability	To which extent is it possible to link a group of transactions to a specific identity?

TABLE IV
SECURITY CONSIDERATIONS FOR BLOCKCHAIN SYSTEMS

from Nakamoto style consensus algorithms for leader election. This scheme allows for immediate finality, which enables consensus algorithms to work in a permissionless setting. The consensus algorithms can scale better than standard Nakamoto consensus algorithms with the cost of reduced Byzantine fault tolerance.

Crash tolerant style consensus algorithms, i.e., Raft, provide consensus in a single communication step, with the optimal communication complexity of $\Theta(n)$. It also provides deterministic finality. The main caveat related to crash tolerant consensus algorithms is that they cannot tolerate Byzantine faults. Disregarding Byzantine faults, Raft tolerates up to 50% crashed nodes. Raft's communication pattern is completely leader-centered. During normal operation, the leader continuously broadcasts messages to the rest of the network, while follower nodes only respond to the messages they receive. Therefore, the leader node must have sufficient network throughput and computational resources for the leader not to become a bottleneck in terms of performance.

B. Integrity

Limited network throughput may cause increased asynchrony within a blockchain system. This makes it infeasible to make assumptions regarding the ordering or timing of messages being sent. As such, consensus algorithms relying on synchronous network for correctness cannot provide integrity in the relevant setting.

Nakamoto style consensus algorithms are unfit for the setting [49].

BFT style consensus algorithms may work depending on their timing assumptions. Linear-BFT specifically assumes synchronous network and therefore cannot guarantee integrity

either. BFT consensus algorithms assuming a partial synchronous or asynchronous network will still provide integrity in such an asynchronous network. It is important to point out that while many BFT style consensus algorithms can provide integrity during times of asynchrony, these same algorithms cannot provide liveness at the same time, as a result of the FLP impossibility [22]. The network needs to stabilize before transactions can be continued to be processed. In light of this, the Honey-BadgerBFT consensus algorithm differentiates itself, as it makes no assumptions regarding the network's synchrony. As Honey-BadgerBFT functions purely asynchronously, it may avoid the standstill of asynchrony or performance impact of a larger message delay Δ . In particular, [43] points out that there will always be an inherent trade-off related to such synchrony assumptions. If the Δ parameter value is too low, the system will not provide progress. If the Δ parameter value is too high, it will not fully take advantage of the network's bandwidth. The authors propose Honey-BadgerBFT as a candidate for consortium blockchain systems, emphasizing its benefits of robustness and high transaction throughput, despite being an asynchronous system.

FBA style consensus algorithms, i.e., RPCA and SCP, assume a partially synchronous network and can provide integrity even in periods of asynchrony. However, they require messages to be bounded by some upper bound message delay Δ to provide forward progress.

Hybrid style consensus algorithms Byzcoin and Tendermint make synchronization assumptions equal to that of partial synchrony. In times of asynchrony, consensus algorithms can preserve integrity. Conversely, the consensus algorithms' transaction throughput may suffer significantly during these events, similar to that of BFT style consensus algorithms.

Name	Ref	Latency	Complexity	Timing assumptions	BFT	Finality
Nakamoto style consensus algorithms						
PoW	[24]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoS	[25]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
DPoS	[26]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
DDPoS	[27]	3 RTT	$\Theta(n^2)$	Synchronous	50 %	Probabilistic
PoAuth	[28]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoET	[29]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoTS	[30]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoR	[31]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoB	[32]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoC	[33]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoI	[34]	1 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
PoA	[35]	3 RTT	$\Theta(n)$	Synchronous	50 %	Probabilistic
BFT style consensus algorithms						
Linear-BFT	[36]	6 RTT	$\Theta(n)$	Synchronous	50 %	Immediate
PBFT	[37]	3 RTT	$\Theta(n^2)$	Partial Synchronous	33 %	Immediate
IBFT	[38]	3 RTT	$\Theta(n^2)$	Partial Synchronous	33 %	Immediate
Delegated BFT	[39]	3 RTT	$\Theta(n)$	Partial Synchronous	33 %	Immediate
BFT - SMART	[40]	3 RTT	$\Theta(n^2)$	Partial Synchronous	33 %	Immediate
T-PBFT	[41]	3 RTT	$\Theta(n^2)$	Partial Synchronous	33 %	Immediate
MBFT	[42]	N/A	$\Theta(n)$	Partial Synchronous	33 %	Immediate
Honey-BadgerBFT	[43]	6 RTT	$\Theta(n^2)$	Asynchronous	33 %	Immediate
Federated Byzantine Agreement consensus algorithms						
RPCA	[44]	N/A	$\Theta(n^2)$	Partial Synchronous	20 %	Immediate
SCP	[45]	N/A	$\Theta(n)$	Partial Synchronous	N/A	Immediate
Hybrid consensus algorithms						
BFT-based POW	[46]	3 RTT	$\Theta(n)$	Partial Synchronous	33 %	Immediate
BFT-based POS	[47]	3 RTT	$\Theta(n)$	Partial Synchronous	33 %	Immediate
Crash Tolerant consensus algorithms						
Raft	[48]	1 RTT	$\Theta(n)$	Partial Synchronous	0 %	Immediate

TABLE V
CONSENSUS ALGORITHM CLASSIFICATION

Crash tolerant style consensus algorithm relies on synchronization assumptions similar to that of BFT style consensus algorithms. In particular, Raft assumes a known broadcasting latency, which is then used to determine an election timeout interval. The algorithm can ensure integrity, even in periods of asynchrony, despite the message delay exceeding the assumed bound. However, it will not be able to provide any forward progress in such events. There will be a continuous re-election process until the network stabilizes. This may be problematic in terms of a network with high communication latency and poor network throughput.

C. Security

Nakamoto style consensus algorithms are targets of a multitude of attacks. Sufficient delay of messages caused by the asynchrony of the network may enable double spend and balance attacks. Furthermore, the Nakamoto style consensus algorithms may be vulnerable to P + Epsilon attacks, depending on the blockchain system's incentivization mechanisms. In contrast to many other types of consensus schemes, which are centered around a stable leader, Nakamoto style consensus algorithms elect leaders non-deterministically on a block-to-block basis, which makes DDOS attacks infeasible in most

practical settings. Conversely, the consensus algorithms may, however, be vulnerable to BGP attacks. In particular, [50] has shown the feasibility of utilizing routing attacks against Bitcoin's PoW scheme.

BFT style consensus algorithms usually have an increased susceptibility towards DDOS attacks, compared to Nakamoto style consensus. Specifically, when sufficiently powerful adversaries have insight into which of the network's nodes is the leader for a given election term or view, they could impair the system's liveness by overloading the leader with incoming traffic. This is exasperated in our SCM setting with low network throughput. As many BFT style consensus algorithms rely on a stable leader for progress, in the worst case, this could lead to a continuous view change, grinding transaction throughput to a halt. The Honey-BadgerBFT consensus algorithm once again differentiates itself from the other BFT style consensus algorithms in that it is leaderless. Therefore, the Honey-BadgerBFT consensus algorithm does not suffer from the aforementioned susceptibility towards DDOS attacks. DDOS attacks could also potentially target non-leader nodes in an attempt to increase the number of faulty nodes. As most BFT style consensus algorithms require a supermajority of honest nodes to ensure the system's integrity, a sufficiently powerful

RQ1: What consensus models are able to provide integrity in an environment with limited network throughput?

Consensus algorithms	Nakamoto	BFT	FBA	Hybrid	Crash Tolerant
Integrity in asynchronous system	-	!	+	+	+

RQ2: What consensus models are able to provide security in an environment with limited network throughput?

Consensus algorithms	Nakamoto	BFT	FBA	Hybrid	Crash Tolerant
Double spend attacks	-	+	+	+	!
Balance attacks	-	+	+	+	+
Long-Range attacks	!	+	+	+	+
P + Epsilon attacks	!	+	+	+	+
DDOS attacks	+	-	!	-	-
BGP attacks	-	-	!	-	-

+ Strong guarantees

- Lacking guarantees

! Depending on the specifics of the consensus algorithm or the configuration of the blockchain system

TABLE VI

SUMMARY OF CONSENSUS ALGORITHMS IN RELATION TO PERFORMANCE METRICS, RQ1 AND RQ2.

adversary could target honest nodes and break the Byzantine Fault Tolerance threshold. Whether this would be feasible in a practical setting depends on the size of the network, the current number of Byzantine nodes, as well as the adversaries' combined computational resources. Linear-BFT, which only requires a majority of honest nodes to ensure integrity, may be better suited to defend against this kind of attack. BFT style consensus algorithms could also be vulnerable to BGP attacks. When an adversary gains control of routing mechanisms used within the system, they could potentially partition the network or delay communication between nodes. Targeting the leader could hamper the liveness of the system. When the adversaries have access to an especially central router within the communication system, they could isolate larger groups of participants. Like a DDOS attack, this could allow adversaries to break the Byzantine Fault Tolerance threshold, invalidating any guarantees about the system's integrity.

FBA style consensus algorithms avoid some of the pitfalls related to BFT style consensus. In particular, as RPCA and SCP are leaderless, there is no vulnerability related to a leader being targeted by a DDOS attack, stopping the system from achieving progress. There is, however, a new potential attack vector related to splitting the network. Going back to the important role in which intersecting nodes play in federated Byzantine agreement, a sufficiently powerful adversary could perform DDOS attacks targeting well-connected nodes. Such an attack could partition the network, isolating nodes, making consensus in the original network unachievable, and hindering transaction throughput. FBA style consensus algorithms could be vulnerable to the BGP attack. Similar to that of a targeted DDOS attack against a well-connected node, if an adversary gains control of a central router within the communication network, they could partition the network, creating divergence. In terms of RPCA, where the 90% UNL overlap makes divergence attacks unlikely, attackers might rather try to break

the Byzantine Fault Tolerance threshold of 20%. As for SCP, allowing users to communicate only with nodes selectively they specifically trust, any form of substantial routing attack may break the network, depending on the size of each user's node list.

Hybrid style consensus algorithms have an increased susceptibility to DDOS attacks due to the transition from Nakamoto style consensus to a hybrid approach. Like BFT style consensus algorithms, the hybrid approach is leader-centered and needs to maintain a stable leader to provide high performance. Combined with limited network throughput, this may further hinder transaction throughput. DDOS attacks might also target non-leader nodes of the network. As inclusion in the inner consensus group is the core of Nakamoto style consensus mechanisms, attacking arbitrary nodes would require most nodes to become faulty before the Byzantine Fault Tolerance threshold would break. If the adversary instead chooses to target the inner consensus group, the threshold is reduced to only 33% of the consensus group itself, and as such, should be significantly more feasible. Furthermore, hybrid style consensus algorithms are vulnerable to BGP attacks. Combining Nakamoto and BFT style consensus mechanisms, Hybrid style consensus algorithms inherit both groups' vulnerabilities related to BGP.

Crash tolerant style consensus algorithm suffers from the same DDOS susceptibility as BFT style consensus algorithms. The consensus algorithm needs to maintain a stable leader to provide liveness, and such, continuous DDOS attacks targeting leaders can hamper transaction throughput. This may be further exasperated by nodes having limited network throughput. Similar to BFT style consensus algorithms, a DDOS attack may also be used against arbitrary network nodes. In Raft's case, to break the Crash Tolerance threshold, a total of 50% of the network nodes must become faulty. Thus, unless the network is volatile and at some points contains a lot of faulty

nodes, such an attack would be less practical than targeting the leader directly. Finally, Raft is also vulnerable to BGP attacks. An adversary initiating a routing attack against the network leader would be able to completely halt transaction throughput, hindering any broadcasts from reaching the follower nodes. Furthermore, given sufficient power, the adversary could partition the network, attempting to break the Crash Tolerance threshold of 50%, enabling double spends.

V. DISCUSSIONS

A. Comparison with related work

Numerous surveys, e.g., [6], [7], [9], [11] have been dedicated to present and classify consensus algorithms according to their performance characteristics. In particular, [6] and [7] present novel evaluation frameworks for analyzing consensus algorithms. [6] furthermore highlights the impact network synchrony has on consensus algorithms. Our study differs from related work because it focuses on consensus algorithms' performance characteristics in the specific application scenario in which the network is constrained by varying network throughput. Furthermore, our classification scheme is skewed towards the impact of communication costs and timing assumptions on the algorithms' performance, utilizing the metrics of communication latency, communication complexity, and timing assumptions.

Studies [6], [11], [12] focuses on the security properties of consensus algorithms, including that of ensuring the integrity of the blockchain. [11] discusses core security properties of consensus algorithms and their ability to ensure consistency and tamper-resistance across a blockchain system's ledgers. [12] furthermore discusses the circumstances in which these properties may be broken. [6] discusses how consensus algorithms may function in a fully asynchronous setting. Our study differentiates from [6], [11], [12] in that it investigates how consensus algorithms ensure integrity in the specific application scenario in which the network is constrained by varying network throughput. The scenario includes both increased asynchrony of the network, as well as isolation of nodes. It thus provides a unique perspective into which consensus algorithms can provide safety and integrity in such a constrained environment.

B. Known limitations

This study does not provide insight into experimental data for the different consensus algorithms surveyed. It is, therefore, difficult to draw comparisons regarding transaction throughput among different categories of consensus algorithms.

Furthermore, this study focuses on consensus in enterprise and permissioned blockchain systems affected by limited network throughput. Blockchain systems that do not fit a similar application scenario may emphasize other factors rather than those presented by our classification scheme. The security aspect of this study is based on the reviews of [11] and [12]. While it is deemed that these works constitute a comprehensive review of security attacks generally applicable to blockchain systems, there may be other security attacks to consider, given

the specifics of the blockchain system in question or the scenario in which it is utilized.

VI. CONCLUSION AND FUTURE WORK

The purpose of this study is to analyze how the state of the art consensus algorithms relate to SCM blockchain systems in an enterprise setting with multiple stakeholders, affected by limited network throughput and poor network quality. The mapping study's classification emphasizes how well the consensus algorithms can satisfy performance, integrity, and security requirements in a degraded network environment. The study gives insights into the advantages and weaknesses of the investigated consensus algorithms. Our future work will evaluate and compare the consensus algorithms identified from this study more quantitatively by running simulations and experiments.

REFERENCES

- [1] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, IEEE, 2016, pp. 1–3.
- [2] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*, Springer, 2016, pp. 239–278.
- [3] A. Stanciu, "Blockchain based distributed control system for edge computing," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, IEEE, 2017, pp. 667–671.
- [4] Y. Chang, E. Iakovou, and W. Shi, "Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities," *International Journal of Production Research*, vol. 58, no. 7, pp. 2082–2099, 2020.
- [5] S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," 2002.
- [6] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, ISSN: 1553-877X. DOI: 10.1109/COMST.2020.2969706.
- [7] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113 385, 2020, ISSN: 0957-4174. DOI: <https://doi.org/10.1016/j.eswa.2020.113385>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0957417420302098>.
- [8] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Future Generation Computer Systems*, vol. 107, pp. 760–769, 2020, ISSN: 0167-739X. DOI: <https://doi.org/10.1016/j.future.2017.09.023>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X17320095>.
- [9] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, "Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review," *IEEE Access*, vol. 7, pp. 43 622–43 636, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2904181.
- [10] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2896108.
- [11] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, Article 51, 2019, ISSN: 0360-0300. DOI: 10.1145/3316481. [Online]. Available: <https://doi.org/10.1145/3316481>.
- [12] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. 9, p. 1788, 2019. DOI: 10.3390/app9091788.

- [13] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019, ISSN: 1553-877X. DOI: 10.1109/COMST.2019.2928178.
- [14] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019, ISSN: 1364-0321. DOI: <https://doi.org/10.1016/j.rser.2018.10.014>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1364032118307184>.
- [15] S. Alsaqqa and S. Almajali, "Blockchain technology consensus algorithms and applications: A survey," *International Journal of Interactive Mobile Technologies (IJIM)*; Vol 14, No 15 (2020), 2020. [Online]. Available: <https://online-journals.org/index.php/i-jim/article/view/15893>.
- [16] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54 371–54 401, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2981415.
- [17] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, Article 18, 2020, ISSN: 0360-0300. DOI: 10.1145/3372136. [Online]. Available: <https://doi.org/10.1145/3372136>.
- [18] A. Pieroni, N. Scarpato, and L. Felli, "Blockchain and iot convergence—a systematic survey on technologies, protocols and security," *Applied Sciences*, 2020.
- [19] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *EASE*.
- [20] *Oria search engine*, Accessed 05.09.2020. [Online]. Available: <http://oria.no/>.
- [21] Hyperledger, "Hyperledger blockchain performance metrics," 2018. [Online]. Available: <https://www.hyperledger.org/learn/publications/blockchain-performance-metrics>.
- [22] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, 374–382, 1985, ISSN: 0004-5411. DOI: 10.1145/3149.214121. [Online]. Available: <https://doi.org/10.1145/3149.214121>.
- [23] C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of partial synchrony," *J. ACM*, vol. 35, no. 2, 288–323, 1988, ISSN: 0004-5411. DOI: 10.1145/42282.42283. [Online]. Available: <https://doi.org/10.1145/42282.42283>.
- [24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, Accessed 05.09.2020.
- [25] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds., Springer International Publishing, pp. 357–388, ISBN: 978-3-319-63688-7.
- [26] D. Larimer, "Delegated proof-of-stake (dpos)," *Bitshare whitepaper*, 2014.
- [27] F. Yang, W. Zhou, Q. Wu, R. Long, N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. PP, Aug. 2019. DOI: 10.1109/ACCESS.2019.2935149.
- [28] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain," *Italian Conference on Cyber Security (06/02/18)*, 2018. [Online]. Available: <https://eprints.soton.ac.uk/415083/>.
- [29] I. Corporation, *Poet 1.0 specification*, <https://sawtooth.hyperledger.org/docs/core/releases/1.0/arch-itecture/poet.html>, Accessed 05.09.2020.
- [30] S. Andreina, J. M. Bohli, G. Karame, W. Li, and G. A. Marson, "Pots: A secure proof of tee-stake for permissionless blockchains," *IEEE Transactions on Services Computing*, pp. 1–1, 2020, ISSN: 1939-1374. DOI: 10.1109/TSC.2020.3038950.
- [31] K. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," *IACR Cryptology ePrint Archive*, vol. 2008, p. 175, 2008.
- [32] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn," in *Financial Cryptography and Data Security*, J. Boneau and N. Heninger, Eds., Springer International Publishing, pp. 523–540, ISBN: 978-3-030-51280-4.
- [33] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Advances in Cryptology – CRYPTO 2015*, R. Gennaro and M. Robshaw, Eds., Springer Berlin Heidelberg, pp. 585–605, ISBN: 978-3-662-48000-7.
- [34] *Nem: Technical reference*, https://nemplatform.com/wp-content/uploads/2020/05/NEM_techRef.pdf, Accessed 05.09.2020.
- [35] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," *SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, 34–37, Dec. 2014, ISSN: 0163-5999. DOI: 10.1145/2695533.2695545. [Online]. Available: <https://doi.org/10.1145/2695533.2695545>.
- [36] A. Momose and L. Ren, "Optimal communication complexity of byzantine consensus under honest majority," *arXiv e-prints*, arXiv:2007.13175, 2020. [Online]. Available: <https://ui.adsabs.harvard.edu/abs/2020arXiv200713175M>.
- [37] M. Castro and B. Liskov, *Practical byzantine fault tolerance*, <http://pmg.csail.mit.edu/papers/osdi99.pdf>, Accessed 05.09.2020.
- [38] H. Moniz, "The istanbul bft consensus algorithm," *arXiv e-prints*, arXiv:2002.03613, 2020. [Online]. Available: <https://ui.adsabs.harvard.edu/abs/2020arXiv200203613M>.
- [39] Q. Wang, J. Yu, Z. Peng, V. C. Bui, S. Chen, Y. Ding, and Y. Xiang, "Security analysis on dbft protocol of neo," 2020. [Online]. Available: <https://fc20.ifca.ai/preproceedings/32.pdf>.
- [40] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with bft-smart," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2014, pp. 355–362.
- [41] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118 541–118 555, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2935149.
- [42] M. Du, Q. Chen, and X. Ma, "Mbft: A new consensus algorithm for consortium blockchain," *IEEE Access*, vol. 8, pp. 87 665–87 675, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2993759.
- [43] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of bft protocols," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, Vienna, Austria: Association for Computing Machinery, 2016, 31–42, ISBN: 9781450341394. DOI: 10.1145/2976749.2978399. [Online]. Available: <https://doi.org/10.1145/2976749.2978399>.
- [44] B. Chase and E. MacBrough, *Analysis of the xrp ledger consensus protocol*, 2018. arXiv: 1802.07242 [cs.DC].
- [45] D. MAZIERES, *Stellar consensus protocol*, <https://www.stellar.org/papers/stellar-consensus-protocol>, Accessed 05.09.2020.
- [46] E. Kokoris-Kogia, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," 2016. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kokori.
- [47] J. Kwon, "Tendermint: Consensus without mining," 2014. [Online]. Available: <https://tendermint.com/static/docs/tendermint.pdf>.
- [48] D. Ongaro and J. Ousterhout, *In search of an understandable consensus algorithm (extended version)*, <https://raft.github.io/raft.pdf>, Accessed 05.09.2020.
- [49] R. Pass, L. Seeman, and A. Shelat, *Analysis of the Blockchain Protocol in Asynchronous Networks*. 2017, pp. 643–673, ISBN: 978-3-319-56613-9. DOI: 10.1007/978-3-319-56614-6_22.
- [50] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392, ISBN: 2375-1207. DOI: 10.1109/SP.2017.29.

This figure "fig1.png" is available in "png" format from:

<http://arxiv.org/ps/2103.02916v1>