Security of Consensus Mechanisms in Blockchain

Mihai BABOI
National Institute for Research and Development in Informatics - ICI Bucharest
mihai.baboi@ici.ro

Abstract: Blockchain technology has gained widespread recognition as a revolutionary decentralized system that offers immutable and secure transaction records. A key element responsible for ensuring the integrity and trustworthiness of blockchain networks is the consensus mechanism. The consensus mechanism defines the rules through which nodes in a distributed network agree on the validity of transactions and maintain a consistent and tamper-resistant ledger. This paper explores the security aspects related to various consensus mechanisms in blockchain and their role in safeguarding the network from potential attacks. Consensus mechanisms play a pivotal role in ensuring coherence and agreement among nodes in distributed systems. These mechanisms enable nodes to collectively determine the state of the system, even in the presence of adversarial behavior. This text delves into the concept of consensus mechanisms, their importance in various contexts, and their role in guaranteeing reliability and trust, supported by insights from academic research.

Keywords: Consensus Mechanisms, security, trilemma, blockchain architecture, attack, Byzantine Fault Tolerance.

INTRODUCTION

Consensus mechanisms are protocols that facilitate agreement among multiple nodes in a distributed system. As Lamport et al. (1982) defines it: „A consensus algorithm allows a collection of processes to work together effectively to reach agreement on a common value." This agreement is vital for maintaining the integrity of the system and ensuring its consistent operation. The security of these consensus mechanisms is of paramount importance, as they dictate the integrity, reliability, and overall trustworthiness of blockchain systems. With various consensus algorithms in use, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and more, understanding and ensuring their security is essential to prevent attacks, maintain network stability, and instill confidence in the broader blockchain ecosystem. As the digital landscape continues to evolve, threats to consensus mechanisms become increasingly sophisticated. Malicious actors seek to exploit vulnerabilities, launch attacks, and compromise the principles that underpin blockchain's promise of security and decentralization. In response, researchers, developers, and practitioners are continuously exploring innovative defense strategies to safeguard against potential risks, enhance a system`s resistance to adversarial behavior, and maintain the credibility of consensus protocols.

https://doi.org/10.54851/v5i2y202305

BLOCKCHAIN TRILEMMA

When talking about consensus mechanisms, one should also refer to security aspects. For this, the blockchain trilemma should be discussed. A fundamental concept in the realm of blockchain technology, it encapsulates the intricate balance between three core attributes: scalability, security, and decentralization. This trilemma underpins the design and operational considerations of blockchain networks, illuminating the challenges faced by architects and developers in optimizing these characteristics. As it was noted by Buterin and others, „blockchains fundamentally suffer from an inherent scalability-security-decentralization trilemma: you can pick any two." (Buterin, 2017). This trilemma underscores the reality that enhancing one aspect inevitably requires compromises in at least one of the other dimensions.

Scalability, the first facet of the trilemma, pertains to the capacity of a blockchain network to process a significant volume of transactions within a specific timeframe. As it was highlighted by Karame et al. (2012) „scalability, the ability to handle a large number of transactions, is an important requirement for public blockchain systems." Achieving high scalability is a persistent pursuit, driven by the demand for blockchain networks to handle an expanding user base and diverse applications. However, the pursuit of scalability often involves trade-offs in security and decentralization, as it was evidenced by the phenomenon that increasing transaction throughput can undermine the time-tested security mechanisms.

Security, the second dimension, stands as a cornerstone of blockchain technology. The immutability and tamper-resistant nature of distributed ledgers are underpinned by robust security protocols and consensus mechanisms. As it was emphasized by (Zohar, 2015): „blockchain technology relies on cryptographic techniques to provide confidentiality, integrity, and authenticity."

The security aspect of the trilemma calls for measures to thwart attacks, prevent fraudulent activities, and ensure the integrity of transactions. Yet, bolstering security can impose constraints on the network's scalability and decentralization.

Decentralization, the final facet, embodies the principle of distributing control and decision-making across a network of participants. As it was expounded by Swan (2015): „decentralization is a critical aspect of blockchain, as it promotes trust in a trustless environment." A decentralized network is more resistant to censorship, central points of failure, and malicious manipulation. However, achieving a high level of decentralization may come at the cost of scalability and security, as the consensus mechanisms required for decentralization could introduce latency and complexities.

The blockchain trilemma's intricate interplay among scalability, security, and decentralization underscores the necessity for a nuanced approach in designing and implementing blockchain networks. As underlined by (Narayanan et al., 2016): „many design choices and trade-offs are influenced by the trilemma." Blockchain projects and researchers are actively engaged in exploring innovative solutions that mitigate the trade-offs, seeking to strike an optimal balance between the three dimensions based on specific use cases and priorities. Ultimately, acknowledging the existence of the trilemma paves the way for a way more informed and thoughtful development of blockchain technology.

BLOCKCHAIN ARCHITECTURE

Before going into detail about some consensus mechanisms, the bigger picture of blockchain architecture should be analyzed. Blockchain technology has evolved into a complex ecosystem that relies on a multi-layered architecture to function efficiently and securely. The architecture presented in Figure 1 and the potential threats that can appear on each individual layer will be analyzed. Each layer of the blockchain architecture, from infrastructure to application, contributes to the overall security posture.

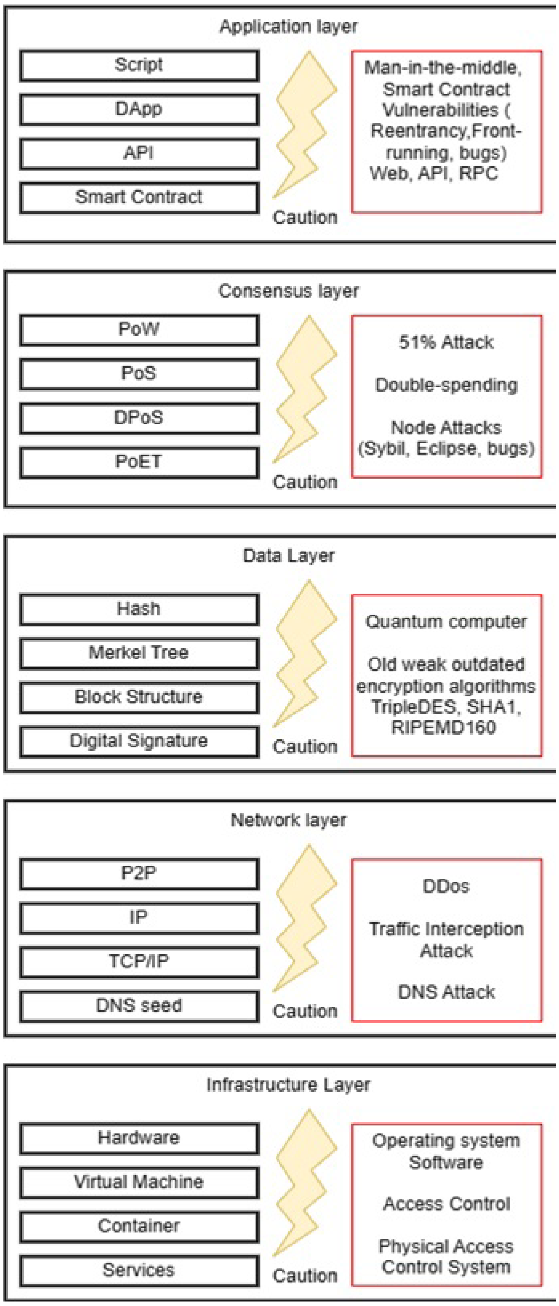

***Figure 1.** Blockchain Architecture*

By fortifying each layer against potential threats and vulnerabilities, blockchain systems can achieve a layered defense that enhances overall security and ensures the continued advancement of this transformative technology.

The infrastructure layer refers to the hardware and software that support blockchain applications to run. This layer can be made up of docking containers, various operating systems that run on premises or on public cloud. Gaining unauthorized access to the operating system or physical access to hardware can affect the node behavior and the network.

The network layer's security hinges on preventing unauthorized access and data tampering. „Security measures at the network layer are crucial to resist attacks like eavesdropping, spoofing, and denial-of-service" (Zheng et al., 2017). Encryption, secure communication protocols, and robust authentication mechanisms within this layer defend against attacks that compromise data integrity during its transmission. DNS seeds attacks can exploit vulnerabilities in the DNS infrastructure to manipulate the peer discovery process. Attackers may attempt to poison or manipulate the DNS records, redirecting new nodes to malicious or controlled peers. By doing so, they can potentially compromise the security and integrity of the blockchain network.

The data layer's security rests upon its immutability and transparency. „Immutability of data helps ensure the integrity of transactions, enabling transparent and tamper-proof records" (Dagher et al., 2018). The decentralized nature of blockchain ensures that data stored in this layer cannot be altered or manipulated without consensus from the majority of nodes. Quantum computing, a rapidly advancing field, holds the potential to disrupt traditional encryption methods that have long been the bedrock of cybersecurity. On the projection steps, old, outdated encryption algorithms can open space for some security problems.

Further on, consensus protocols lie at the heart of decentralized systems, facilitating agreement among distributed nodes to validate transactions and maintain the integrity of shared ledgers. These protocols are the cornerstone of blockchain networks, ensuring trust and reliability without the need for intermediaries. The security of this layer is very important because „Consensus protocols prevent adversaries from sending transactions that spend the same coins twice" (Gervais et al., 2016). The consensus layer provides security by preventing malicious activities such as double-spending, 51% attacks and Sybil attacks that will be detailed later in this article. Byzantine

Fault Tolerance (BFT) and Proof of Work (PoW) algorithms within this layer ensure that a majority of honest nodes overpower adversaries, fortifying the network against malicious intent.

The application layer's security focus is on safeguarding user data and interactions. Robust authentication, authorization, and access control mechanisms within this layer protect user information and interactions, maintaining confidentiality and privacy. „The application layer hosts decentralized applications (DApps) and provides the interface for users and applications to interact with the blockchain" (Zheng et al., 2017). DApps include a wide range of functionalities from finance and supply chain management to identity verification and voting systems. The complexity of smart contracts can introduce vulnerabilities due to coding errors. As Atzei warns: „Smart contracts can suffer from vulnerabilities that may lead to significant financial losses" (Atzei et al., 2017). Smart contracts have the potential to revolutionize various industries, but their vulnerabilities are a significant concern. There will always be risks associated with coding errors, reentrancy attacks, integer overflows, and unchecked external calls. Secure smart contract development practices, stringent audits, and ongoing research are essential for mitigating vulnerabilities and building a resilient blockchain ecosystem. As all interactions use API (Application Programming Interface), RPC (Remote procedure call), and web infrastructure, all known OWASP (https://owasp.org) recommendations will apply.

Ensuring the security of blockchain application architecture layers is a complex undertaking that necessitates meticulous attention and a holistic strategy. Academic insights underscore the significance of securing user interactions, business logic, data access, smart contracts, and external service integration. A secure blockchain system relies on the protection of each architecture layer. Understanding the nuances of the blockchain infrastructure architecture layers is essential for architects, developers, and researchers seeking to design and optimize blockchain networks that are resilient, scalable, and capable of revolutionizing various domains.

Blockchain consensus mechanisms play a pivotal role in achieving agreement and maintaining the integrity of decentralized networks. These mechanisms determine how consensus is reached among distributed nodes, ensuring the reliability and security of blockchain systems. This essay delves into the intricacies of blockchain consensus mechanisms, drawing insights from academic sources to illuminate their diverse approaches and implications. These protocols enable distributed nodes to agree on the state of the blockchain. „Consensus protocol is the key technology that enables blockchain's decentralization, or more specifically, that ensures all participants agree on a unified transaction ledger without the help of a central authority„ (Xiao et al., 2020) These mechanisms underpin the decentralized nature of blockchain networks. Further on, this paper will detail the consensus mechanisms, its advantages and disadvantages, and its weaknesses and strengths.

CONSENSUS MECHANISMS

Proof of Work is one of the most renowned consensus mechanisms, introduced by Nakamoto (2008) in the context of Bitcoin. He explained that PoW „requires miners to solve computational puzzles to add blocks to the blockchain", thereby ensuring the network's security through energy-intensive calculations. However, the energy consumption and the possibility of a 51% attack pose concerns. While challenging, the likelihood of such an attack decreases as the network grows larger, bolstering security. However, PoW is energy-intensive and susceptible to the 51% attack, where a malicious entity gains control over the majority of the network's computing power and can manipulate transactions or commit double-spending attacks. While the 51% attack is theoretically possible, in practice, it becomes increasingly difficult as the network's size and computing power grow (Eyal & Sirer, 2014).

Proof of Stake is an alternative consensus mechanism that addresses the energy consumption issues of PoW.

In PoS, validators are chosen to create blocks and verify transactions based on the number of coins they „stake" or „lock up" as collateral. Validators with higher stakes have a higher probability of being chosen. PoS is considered more secure since it requires a substantial financial investment to attack the network successfully. However, PoS is not entirely immune to attacks, particularly the „nothing at stake" problem. In this scenario, validators might try to create multiple blockchain forks simultaneously, as there is no cost associated with doing so. To mitigate this, many PoS blockchains implement mechanisms to penalize validators who act maliciously and encourage them to remain honest.

PoS offers several advantages over PoW, including energy efficiency, scalability, and reduced centralization risks. As Buterin notes, „Proof of Stake algorithms are faster and significantly more energy-efficient than Proof of Work algorithms." (Buterin et al., 2019) Additionally, PoS mitigates the threat of centralization posed by large mining operations. Despite its benefits, PoS is not without challenges. The distribution of stake, potential for long-range attacks, and „nothing at stake" problem are areas of concern. As Babaioff cautions, „Proof of Stake protocols are not immune to attacks and vulnerabilities." (Babaioff, 2012). Ensuring a fair distribution of stake and addressing potential vulnerabilities require a careful design and ongoing research. Security in Proof of Stake networks requires Byzantine Fault Tolerance (BFT) mechanisms; „Ouroboros, a PoS protocol, provides a provably secure blockchain protocol based on a rigorous security model for BFT." (Kiayias et al., 2017) BFT ensures consensus even in the presence of malicious nodes, safeguarding the integrity of the blockchain. Proof of Stake presents an intriguing security paradigm, aligning validators' interests with network stability through economic incentives. While challenges like the „Nothing at Stake" problem exist, academic insights highlight mitigation strategies such as slashing conditions. Moreover, Byzantine Fault Tolerance mechanisms reinforce security in PoS networks. As blockchain ecosystems evolve, understanding and enhancing the security of the Proof of Stake mechanism remains a priority to ensure robust and reliable decentralized systems.

Delegated Proof of Stake (DPoS) is a consensus mechanism that has garnered attention for its efficient approach to achieving consensus within blockchain networks. DPoS relies on delegates elected by token holders to validate transactions, offering scalability and governance benefits. This text delves into the intricacies of Delegated Proof of Stake, drawing insights from academic sources to highlight its design, advantages, challenges, and implications. In DPoS, delegates' roles extend beyond validation; they participate in network governance. This democratic approach empowers participants to influence the blockchain's evolution while ensuring efficient transaction processing. DPoS offers several advantages, including fast transaction confirmation and resource efficiency. „DPoS consensus achieves higher throughput compared to traditional PoW and PoS" (Chen et al., 2022). The reduced number of validating nodes and efficient consensus mechanism contribute to an improved scalability and lower energy consumption. Despite its benefits, DPoS faces concerns related to centralization. „DPoS may compromise decentralization since a small number of delegates control the network" (Chen et al., 2022). Mitigation of malicious behavior in DPoS often involves slashing conditions, which means that delegates risk losing their staked tokens as penalties for misbehavior. „Validators are required to deposit a stake and can lose it if they are caught attempting to cheat" (Zamfir, 2018). Slashing conditions increase accountability and discourage malicious activities.

There are various "Proof of" algorithms that are trying to pick validators based on various wages. Proof of Authority (PoA) relies on trusted validators who are identified and authorized to create new blocks. This mechanism is often used in private or consortium blockchains. Proof of Space (PoSpace) requires participants to prove that they have allocated a certain amount of disk space over time. This approach is energy-efficient compared to PoW, but relies on storage capacity. Proof of Burn (PoB) involves participants sending tokens to a verifiably unspendable address, essentially „burning" them.

This demonstrates commitment to the network and is often used to distribute new tokens in a fair manner. Proof of Elapsed Time (PoET) is a consensus mechanism that relies on a trusted execution environment (TEE) to select a leader node for block creation in a randomized manner. Proof of Weight (PoWeight) combines elements of PoW and PoS. It considers both the computational power of miners and the number of coins they hold to determine block creation. Proof of Identity (PoI) requires participants to prove their real-world identity before participating in the consensus process. It aims to prevent Sybil attacks by ensuring that each identity is represented only once. Proof of History (PoH) establishes a verifiable order of events in a blockchain network, aiding to achieving consensus. It is often used in combination with other consensus mechanisms. However, these consensus mechanisms have not been sufficiently studied by the security research community to find their vulnerabilities. It can be stated that one of the most serious security challenges posed by these algorithms can be represented by lower nodes in the network (for smaller networks) that can be open to attack by injected malicious nodes (with an affordable price) that will take control over the network.

Blockchain networks rely on various chosen consensus mechanisms to provide a secure and trustworthy transaction validation. The integration of defense mechanisms within these protocols of consensus mechanisms, such as computational puzzles, economic incentives, slashing conditions, cryptographic signatures, and redundancy, ensures the resilience of the network against a range of attacks. Understanding the intricacies of these defense mechanisms empowers blockchain architects and researchers to choose, develop, and deploy consensus protocols that safeguard the integrity of a decentralized ecosystem.

DEFENSE MECHANISMS

Byzantine Fault Tolerance (BFT) is a critical concept in distributed systems, ensuring resilience against malicious or faulty nodes. BFT mechanisms play a vital role in maintaining the integrity and security of blockchain networks and other decentralized platforms. Byzantine Fault Tolerance aims to guarantee consensus even in the presence of Byzantine faults, where nodes act maliciously or exhibit erratic behavior. Castro & Liskov (2018) elucidated that BFT „enables a set of nodes to reach consensus on a value even if some nodes are malicious." This security measure ensures the network's continued operation despite potential attacks. BFT is a consensus mechanism ensuring reliability in distributed systems despite malicious or faulty nodes. Nodes communicate, propose values, and vote on decisions. A quorum of correctly functioning nodes is required for consensus, preventing a small group of malicious nodes from dominating. BFT uses cryptographic signatures to verify messages, thereby identifying Byzantine nodes. Once a quorum agrees on a value, it's finalized and executed. BFT underpins systems like blockchain, where integrity is vital amid adversarial behavior, ensuring that consensus can be reached even when a fraction of nodes act maliciously or unpredictably.

RBFT or Redundant Byzantine Fault Tolerance is an advanced consensus mechanism that builds upon the principles of Byzantine Fault Tolerance (BFT). RBFT is designed to enhance the security and reliability of distributed systems by introducing redundancy in the consensus process. RBFT expands on the traditional BFT model by introducing redundancy in the form of multiple consensus subprotocols. This approach allows the network to tolerate a higher number of faulty nodes or malicious actors while still achieving consensus. Through redundancy, RBFT aims to improve the system's resilience against various attack vectors and faults. The concept of redundancy is not new in distributed systems. „Redundancy can be used to mask faults, providing a level of fault tolerance that can make the system appear to be highly available even in the presence of failures". (Adya et al., 2002) RBFT leverages this principle by introducing multiple redundant consensus paths, each contributing to the overall fault tolerance of the network. RBFT's redundancy-driven approach offers enhanced security by making it significantly harder for malicious nodes to manipulate the consensus outcome.

"A Byzantine quorum system provides robustness against up to (n - 1)/3 faults, where n is the total number of nodes." (Cachin, 2016) With redundant subprotocols, RBFT can withstand a higher number of malicious nodes while maintaining a consensus decision. RBFT's redundancy-based defense mechanisms have the potential to address challenges posed by Byzantine attacks, network partitions and unexpected node behavior. However, implementing and managing multiple concurrent subprotocols also introduces complexities in terms of communication overhead, synchronization and overall system performance.

HoneyBadgerBFT introduces a defense mechanism known as asynchronous consensus, thereby enabling agreement (consensus between network participants) without requiring synchronized network timing. It employs cryptographic techniques like threshold signatures and encryption to ensure security against network adversaries and potential message manipulation. While HoneyBadgerBFT offers advanced security through its asynchronous nature, it's important to acknowledge potential threats such as Sybil attacks, malicious nodes, and communication disruptions. The foundation of Honey Badger FTs security rests on cryptographic techniques. Employing strong hashing algorithms, digital signatures, and encryption ensures the integrity, authenticity, and confidentiality of data exchanged between nodes, HoneyBadgerBFT extends beyond the consensus algorithm itself. Robust cryptographic practices guard against message tampering and unauthorized access. Ensuring the legitimacy of peers participating in the HoneyBadgerBFT network is crucial. Employing peer validation mechanisms, cryptographic certificates, and public key infrastructure strengthens the defense against malicious actors attempting to join the network. As blockchain technology advances, HoneyBadgerBFT stands as a significant contribution to achieving robust consensus in distributed systems. However, its security must be continuously evaluated and fortified against evolving threats. By employing cryptographic techniques, network security measures, peer authentication, continuous monitoring, and community collaboration, HoneyBadgerBFT can maintain its position as a secure and reliable consensus protocol, contributing to the growth of secure decentralized applications. Different consensus mechanisms offer varying trade-offs between security, scalability, and energy efficiency. Many hybrid consensus mechanisms blend the strengths of multiple protocols to create defense mechanisms tailored to specific use cases. These hybrids aim to strike a balance between security and performance.

DDoS attacks flood a network with a massive volume of traffic, rendering it unable to respond to legitimate requests. In the context of blockchains, DDoS attacks can target nodes, transaction processing, or consensus mechanisms, disrupting network operations and potentially compromising data integrity. Continuous network monitoring and traffic analysis are essential components of DDoS defense. Anomaly detection mechanisms can identify abnormal patterns, allowing administrators to respond proactively and mitigate the impact of attacks before they escalate. Blockchain's inherent decentralization and peer-to-peer architecture provide some natural resilience against DDoS attacks. Attackers must target multiple nodes across the network, which can be challenging given the distributed nature of blockchain systems. Some blockchains implement consensus mechanisms that inherently resist DDoS attacks. Delegated Proof of Stake (DPoS), for instance, introduces voting and reputation systems that discourage malicious actors from disrupting the network. Implementing traffic filtering and rate limiting mechanisms helps differentiate legitimate traffic from malicious requests. By setting thresholds for incoming traffic and blocking suspicious sources, blockchain networks can reduce the success rate of DDoS attacks.

Security defenses differ also across different blockchain network types like public, private, and consortium networks. Public blockchain networks, characterized by their open participation and decentralization, have gained immense popularity for their transparency and immutability. However, these networks are not immune to security threats.

Public blockchains often incorporate economic incentives to encourage honest participation and discourage malicious behavior. Token rewards for miners or validators align participants' interests with network security, ensuring the network's integrity and robustness. Private blockchain networks restrict participation to a selected group of participants. Security focuses on ensuring data privacy, network integrity, and access control. Robust authentication, encryption, and network segmentation prevent unauthorized access and maintain data confidentiality. Consortium blockchain networks involve a group of known and trusted participants collaborating on a shared network. Security revolves around maintaining consensus and managing permissions among consortium members. Robust governance models, consensus protocols, and access controls are vital to prevent malicious behavior and ensure network stability.

CONCLUSION

Blockchain networks rely on various chosen consensus mechanisms to provide a secure and trustworthy transaction validation.

The integration of defense mechanisms within these protocols, such as computational puzzles, economic incentives, slashing conditions, cryptographic signatures, and redundancy, ensures the resilience of the network against a range of attacks. Understanding the intricacies of these defense mechanisms empowers blockchain architects and researchers to choose, develop, and deploy consensus protocols that safeguard the integrity of a decentralized ecosystem. In the course of this analysis, it has become evident that a comprehensive security approach encompasses cryptography, network resilience, economic incentives, and continuous monitoring. The dynamic nature of blockchain security necessitates not only a deep understanding of potential risks but also the capability to counter emerging threats.

The diverse landscape of consensus algorithms, each with its strengths and vulnerabilities, underscores the multifaceted nature of the security challenge. From the energy-intensive Proof of Work (PoW) to the energy-efficient Proof of Stake (PoS), and from Byzantine fault-tolerant protocols to newer paradigms like HoneyBadgerBFT, the overarching goal remains the same: to establish trust in a trustless environment.

ACKNOWLEDGMENT

The research for this article was conducted within the project „Resilient and Interoperable Communication Systems based on Distributed Technologies and Self-Sovereign Digital Identity (RoDID)," funded by the Advanced Research Program based on Emerging and Disruptive Technologies - Support for the Society of the Future (FUTURE TECH).

REFERENCE LIST

Adya, A., Howell, J., Theimer, M., Bolosky, W. J., Douceur, J. R., & Theimer, M. (2002) *Cooperative Task Management without Manual Stack Management*. Proceedings of the Fifth Symposium on Operating Systems Design and Implementation, OSDI '02, 9-11 December 2002, Boston, Massachusetts, USA. Berkeley, California, USA, USENIX Association, pp. 289-302.

Atzei, N., Bartoletti, M. & Cimoli, T. (2017) *A survey of attacks on Ethereum smart contracts. Journal of Cryptocurrency Engineering and Applications*. Proceedings of the 6th International Conference on Principles of Security and Trust, POST 2017, 22-29 April 2017, Uppsala, Sweden. (Part of the Lecture Notes in Computer Science book series, LNSC, volume 10204) Berlin, Springer. pp. 164-186.

Babaioff, M., Dobzinski, S., Oren, S. & Zohar, A (2012). *On Bitcoin and Red Balloons*. Proceedings of the 13th ACM conference on electronic commerce. 56-73.

Buterin, V. (2017) *The Meaning of Decentralization*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [Accessed 24th October 2023]

Buterin, V., Griffith, V. & Wilcke, M. (2019) *Ethereum's Hybrid Casper FFG (v0.1)*. https://eips.ethereum.org/EIPS/eip-1011 [Accessed 24th October 2023]

Cachin, C. (2016) *Architecture of the Hyperledger Blockchain Fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, DCCL 2016, 25 July 2016, Chicago, Illinois, USA. 310, 4.

Castro, M. & Liskov, B. (1999) *Practical Byzantine Fault Tolerance*. Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI '99, 22-25 February 1999, New Orleans, USA. Berkeley, California, USA, USENIX Association. pp. 173-186.

Chen, Y., Liu, F. (2022) Research on improvement of DPoS consensus mechanism in collaborative governance of network public opinion. *Peer-to-Peer Networking and Applications*. 15, 1849–1861.

Dagher, G. G., Mohler, J., Milojkovic, M., Marella, P. B., & Ancillotti, E. (2018) Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*. 39, 283-297.

Eyal, I. & Sirer, E. G. (2014) *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*. Christin, N and Safavi-Naini, R. (eds.) 18th International Conference on Financial Cryptography and Data Security, FC 2014 , 3-7 March 2014, Christ Church, Barbados. (Part of the Lecture Notes in Computer Science book series, LNSC, volume 8437) Berlin, Springer. pp. 436-454.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H. & Capkun, S. (2016) *On the Security and Performance of Proof of Work Blockchains*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, 24-28 October 2016, Vienna, Austria. New York, NY, Association for Computing Machinery. pp. 3-16.

Karame, G., Androulaki, E. & Capkun, S. (2012) *Double-spending fast payments in bitcoin*. CCS'12: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 906–917

Kiayias, A., Russell, A., David, B. & Oliynykov, R. (2017) *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. Annual International Cryptology Conference, CRYPTO 2017, 20-24 August 2017, Santa Barbara, CA, USA. (Part of the Lecture Notes in Computer Science book series, LNSC, volume 10401) Berlin, Springer. pp. 357-388.

Lamport, L., Shostak, R. & Pease, M. (1982) The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*. 4(3), 382-401.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/en/bitcoin-paper. [Accessed 24th October 2023]

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. *Princeton University Press*.

OWASP Foundation. (n.d.) *OWASP Foundation, the Open Source Foundation for Application Security*. https://owasp.org/ [Accessed 24th October 2023]

Swan, M. (2015) Blockchain: Blueprint for a New Economy. *O'Reilly Media*, Sebastopol.

Xiao Y, Zhang N, Lou W, Hou YT (2020). **A survey of distributed consensus protocols for blockchain networks**. *IEEE Commun. Surv. Tut.* 22(2), 1432-1465.

Zamfir, V., Bansal, N., & Sergey, I. (2018). Casper the Friendly Finality Gadget. *Cryptology ePrint Archive*.

Zohar, A. (2015) Bitcoin: Under the Hood. *Communications of the ACM*. 58(9), 104-113.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017) An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE Transactions on Big Data*.