International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Proof of Credibility: A Dynamic Consensus Framework for Blockchain Applications

Khamar Jalpa*[1], Hiren Patel[2]

Submitted: 27/12/2023 **Revised**: 03/02/2024 **Accepted**: 11/02/2024

Abstract: Blockchain is a technology for decentralized data management that was first created for Bitcoin. It is well-liked because of its security, anonymity, and data integrity. Blockchain peers are able to agree thanks to various algorithms. Nevertheless, validatorstatus, latency, and node failure factors are found to be absent from so many current systems. Traditional consensus mechanisms often solely consider technical specifications or stake, neglecting the reputation and credibility of validators. This can lead to malicious actors or less credible validators participating in the network, potentially compromising its integrity and stability. Also, slow transaction processing speeds can hinder user experience and limit blockchain applicability in fast-paced scenarios. Optimizing consensus mechanisms for speed while maintaining security and accuracy remains a significant challenge. Blockchain resilience hinges on its ability to withstand node failures without compromising data integrity or transaction processing. Existing approaches may not adequately address potential failure scenarios, leading to network disruptions and compromised trust. Our novel Proof of Credibility (PoC) tackles key gaps in existing consensus mechanisms, like validator reputation and latency. PoC prioritizes trustworthy validators and optimizes performance, making it ideal for crucial sectors like finance and smart contracts. By analyzing existing mechanisms and their variables like energy consumption and network size, we unveil optimization potential for a new generation of secure, scalable, and future-proof blockchains.

Keywords: *Blockchain, Consensus, Credibility, Decentralization, security*

1. Introduction

Consensus in the context of Blockchain technology refers to the process by which various nodes or participants in a distributed network come to an understanding on the current state of the ledger or the legitimacy of transactions. The block to the chain was first introduced by a group of researchers in 1991 [1]. Every participant in a Blockchain maintains a duplicate of the same ledger, and any new transaction must first be approved by many nodes before it can be added to the ledger. Consensus procedures ensure that only legitimate transactions are added and that everyone agrees on the ledger's current state and some are working on Blockchain applicability in non-digital currency such as application of Blockchain in smart city [7].

With blockchain technology, various consensus techniques are employed, and the choice of the consensus mechanism is determined by the unique needs of the Blockchain network. Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance are a few of the well-known consensus algorithms utilized in Blockchain (BFT).

Participants in a POW consensus mechanism compete to solve a cryptographic puzzle, with the first person to do so receiving fresh cryptocurrency. Blockchain technology has gained the attention of the academic and industrial sectors [2]. This procedure is energy-intensive and secure because it needs a lot of computer power.

The Blockchain is a decentralized, distributed ledger used to record transactions between two parties in a secure, transparent and immutable manner [3]. Participants in a PoS consensus process stake their cryptocurrency to confirm transactions and build new blocks. Less energy is used in this procedure, but participants must have a large amount of cryptocurrency. And the idea of Blockchain was mostly not in use until it was first referred by Satoshi Nakamoto [1].

Participants in a DPoS consensus mechanism choose a small number of nodes to validate transactions on their behalf, accelerating and streamlining the process. All participants in a BFT consensus process must concur on the ledger's current state, even if some nodes are malfunctioning or malevolent. This slows down the process while increasing security. Consensus, in general, is a crucial component of Blockchain technology because it guarantees the transparency and integrity of the ledger and enables users to put their trust in the Blockchain network without depending on a central authority.

2. Analysis of Consensus Algorithms in Distributed ledger

The ever-evolving landscape of blockchain consensus

[1] *LDRP-ITR,Kadi Sarva Vishwavidyalaya,SVKM,Gandhinagar-382015,Gujarat,India*
ORCID ID : 0000-0003-4724-7222
[2] *VS-ITR, Sarva Vidyalaya Kelvani Mandal, Kadi, 382715, India*[3]
** Corresponding Author Email: khamarjalpa7@gmail.com*

mechanisms is a testament to the relentless pursuit of a perfect harmony between security, efficiency, and scalability. While Byzantine Fault Tolerance and Proof of Work have served as foundational pillars, their limitations have birthed a vibrant tapestry of novel approaches. YAC's real-time voting waltz ensures lightning-fast transaction validation, while RDV-Register's "Deposit and Vote" sidesteps the energy-guzzling tango of mining, ideal for the frugal steps of IoT devices. PoM streamlines private blockchain operations, optimizing the rhythm of consensus for maximum efficiency. POSTER's Proof of Probability pirouettes around the pitfalls of both PoW and PoS, offering a captivating new choreography.

Sleepy consensus embraces an unconventional duet, where a watchful minority safeguards the blockchain's security while the majority slumbers peacefully. MBFT's layered and fragmented approach combines existing techniques for a more resilient ensemble, while Ouroboros Genesis facilitates graceful on boarding with minimal information. Finally, PoC Proof of Contribution reimagines the PoW and PoS routines, rewarding good behavior and penalizing missteps, all within the elegant confines of a stake-based system. These are just a few graceful leaps in the consensus waltz, each step propelling us closer to a future where blockchains move seamlessly to the rhythm of innovation.

3. Unveiling the Building Blocks of Blockchain

Blockchain technology has taken the world by storm, captivating organizations and individuals alike with its potential to revolutionize various industries. While the concept of decentralization itself isn't entirely new, blockchain offers a groundbreaking way to implement it, making it understandable why it's gaining so much traction.

To truly grasp the power of blockchain, let's break down its core components:

1. Distributed Ledger: Imagine a shared notebook, accessible to everyone in a network, where every transaction or event is meticulously recorded. That's essentially what a blockchain is—a distributed ledger that stores data in a series of blocks, each linked to the one before it through a unique cryptographic fingerprint called a "hash." This creates an unshakeable chain of evidence, making it virtually impossible to tamper with or erase past records.

2. Peer-to-Peer Network: Unlike traditional systems with a central authority, blockchain operates through a decentralized network of computers, eliminating the need for intermediaries. Each node in the network holds a copy of the entire ledger, ensuring transparency and redundancy. This eliminates single points of failure and empowers participants to directly interact with each other.

3. Blocks: Think of these as the individual pages of the shared notebook. Each block contains a batch of transactions and links to the previous block using its hash. This creates an immutable chain, where altering any data in a block would require recalculating the hashes of all subsequent blocks, an incredibly complex and impractical task.

4. Cryptography: This is the magic sauce that binds everything together. Blockchain leverages sophisticated cryptographic techniques like hashing and digital signatures to secure data and transactions. Hashing ensures data integrity, while digital signatures authenticate ownership and prevent unauthorized modifications.

5. Consensus Mechanism: With numerous nodes in the network, how do they agree on the validity of transactions and the state of the ledger? This is where consensus mechanisms come in. These algorithms define the rules for adding new blocks to the chain and ensure everyone in the network agrees on the same version of the truth.

By understanding these fundamental building blocks, you'll be well on your way to demystifying the intricacies of blockchain technology and its potential to reshape various industries, from finance and healthcare to supply chain management and voting systems

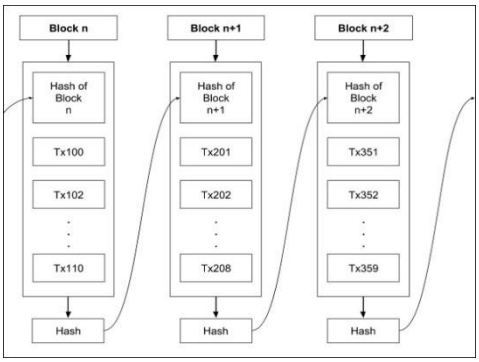


Fig 1 Chain of Blocks in Blockchain

By understanding these fundamental building blocks, you'll be well on your way to demystifying the intricacies of blockchain technology and its potential to reshape various industries, from finance and healthcare to supply chain management and voting systems.

4. Navigating the Blockchain Jungle: Permissioned vs. Permissionless

When it comes to blockchains, not all jungles are created equal. Just like with real forests, you've got your open-door policy permissionless blockchains where anyone can join the party, and then there's the private club of permissioned blockchains with a strict dress code.

Permissionless Powerhouses: Imagine a global bazaar

buzzing with activity. Bitcoin's Proof of Work (PoW) is like the burly gatekeeper, demanding miners solve puzzles to earn the right to add a transaction to the ledger. It's slow, sure, but super secure. Then there's Proof of Stake (PoS), the slick newcomer who lets you stake your coins for a shot at block-building, saving energy in the process. Delegated Proof of Stake (DPoS) throws a twist, putting elected delegates in charge of validation, speeding things up even further.

Consortium Clubs: Now, picture a swanky speakeasy with velvet ropes and a limited guest list. Consortium blockchains are exactly that – exclusive networks for specific industries or organizations. They use clever consensus mechanisms like Raft, a lightning-fast algorithm perfect for private parties, or Byzantine Fault Tolerance (BFT), the ultimate bodyguard against malicious actors. Think PBFT, the tried-and-tested veteran, or DBFT, its delegated cousin, where trusted bookkeepers call the shots.

Beyond the Binary: Remember, the blockchain jungle isn't black and white. Hybrids lurk in the shadows, blending PoW and PoS for double the strength, or Proof of Burn, where participants "sacrifice" coins to earn voting rights. It's a constant quest for the perfect balance between security, speed, and energy efficiency.

So, before you venture into the blockchain wilderness, choose your path wisely. Do you want the wild freedom of a permissionless network or the controlled environment of a consortium club? Whatever your choice, remember, understanding the different types of blockchains is key to unlocking their true potential.

5.Our Novel Proof of Credibility (PoC): Building Trust in Private Blockchains

While existing consensus mechanisms offer valuable solutions for blockchains, they often overlook crucial factors like validator reputation, node resilience, and real-world dynamics. Our proposed Proof of Credibility (PoC) algorithm directly addresses these gaps, building a robust and trustworthy foundation for private blockchains.

Here's what sets PoC apart:

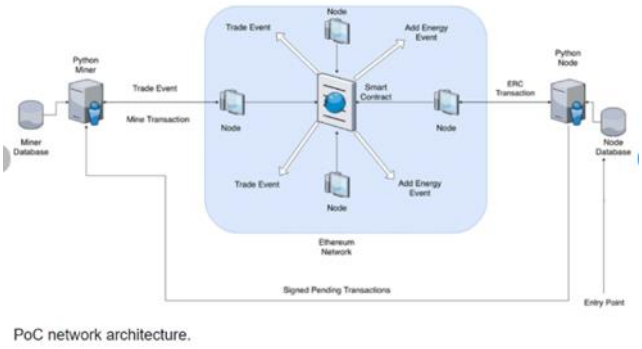
1. Trust, Not Just Tech: PoC moves beyond traditional metrics like computational power or stake, prioritizing the reputation and credibility of validators. Each node accumulates a dynamic credibility score based on its past performance, rewarding consistent accuracy and penalizing misconduct. This score plays a key role in block validation and consensus, promoting a more reliable and trustworthy network.

2. Active vs. Absent: Contrary to the assumption of constant node activity, PoC acknowledges the realities of real-world networks. We implement a node monitoring system that frequently checks node availability through "pinging." Inactive nodes are flagged and excluded from the current consensus round, ensuring only active and engaged participants contribute to block validation.

3. Fault Tolerance: PoC anticipates and handles diverse potential issues including node failures, link failures, and varying computational speeds. Nodes exceeding a predetermined inactivity threshold are marked as failed and communication is suspended. Upon resuming activity, these nodes must undergo re-registration, maintaining network integrity and preventing malicious activity from compromised nodes.

4. Decentralization in Action: PoC actively combats the potential for centralization by mitigating the risk of a few powerful nodes controlling the network. Through dynamic credibility scores and continuous monitoring, PoC empowers more diverse validators to participate in consensus, promoting a more balanced and equitable distribution of power.

Figure 2 illustrates the flow of information, interactions between nodes, and the role of the credibility score within the network architecture.



PoC network architecture.

Fig 2 Proposed Architecture

Depict the mathematical or algorithmic model underlying the credibility score calculation and its impact on consensus decision-making.

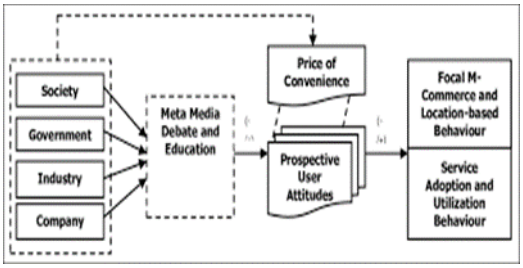


Fig 3 An PoC Model

Figure 4 shows the step-by-step sequence of events during block validation and consensus, highlighting the role of node monitoring and credibility in each stage.

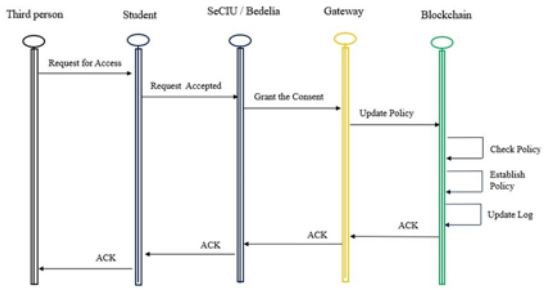


Fig 4 Sequential flow of Block events

6. Modelling and Analysis

Getting agreement on the status of transactions is crucial in the world of blockchain. Reputation based Proof of Credibility, the suggested consensus method, is a scalable and effective solution that enables a large number of nodes to take part in the consensus process. We examined variables including scalability, latency, and throughput to assess the algorithm's performance. Evaluating the performance of the Reputation-based Proof of Credibility (PoC) algorithm demanded a multi-faceted approach. We delved into its scalability, latency, and throughput through a battery of tests and analyses. To gauge its scalability, we employed simulation frameworks that modeled network growth under varying loads. This allowed us to observe how the algorithm's capacity estimation method maintained efficient transaction processing as the network expanded. We also monitored latency, the time it takes for transactions to be confirmed. This involved pinpointing factors like cluster size, message propagation, and validation complexity that influenced confirmation speed. Finally, we assessed throughput, the number of transactions processed per second, using benchmark tools and real-world workload models. This provided insights into the algorithm's ability to handle high transaction volumes under various conditions. By scrutinizing each aspect, we were able to build a comprehensive picture of the PoC algorithm's performance strengths and potential limitations.

Low latency means messages zip around the network faster, letting nodes validate transactions quicker. This cuts down the waiting time for confirmation, like a speedy green light for your transaction to zoom through! Scalability is important since it affects the network's capacity to accommodate the volume of transactions that consumers demand. Even if the network's size or traffic grows, the algorithm can still handle transactions thanks to its capacity estimation method. The length of time it takes the network to confirm a transaction is known as latency. The network can complete transactions more quickly the lower the latency. The number of transactions that may be handled per second, or TPS, is the last unit of measurement used to describe throughput. A high TPS shows that the network can process a lot of transactions in a short amount of time. Our analysis revealed that the PoC algorithm has great scaling, low latency, and high throughput, making it a suitable choice for blockchain consensus. Using client signatures and timestamps, the system we have created enables transactions to be started by nodes and validated by cluster nodes. In the event that the verification is successful, the transaction is passed on to the cluster's master node, where it is confirmed once more before being recorded.

To test our PoC algorithm, we built a mini-blockchain in a controlled environment. Virtual nodes sent transactions, while performance metrics like speed and capacity were monitored. This let us see how PoC handled growing workloads and confirmed transactions quickly, showcasing its potential for real-world blockchains. Future versions could even test resilience to attacks and real-world applications.

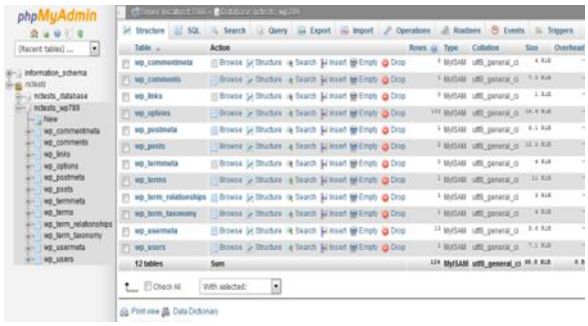


Fig 5 Database design

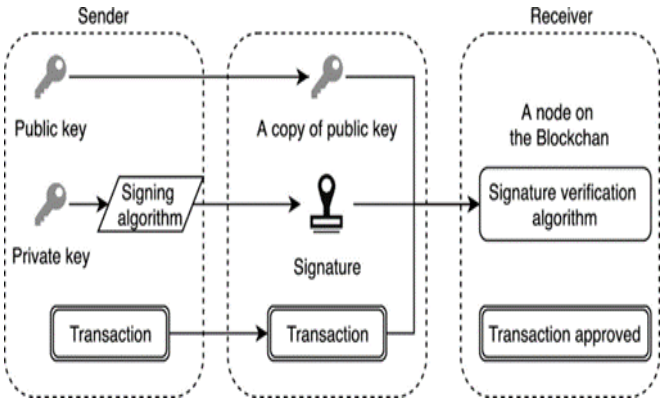


Fig 6 Blockchain-based task and Information Management

We got the following results with context to throughput and latency in comparison to PoW.

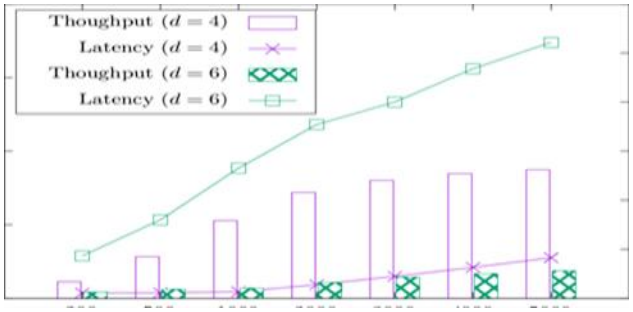


Fig 7 Throughput

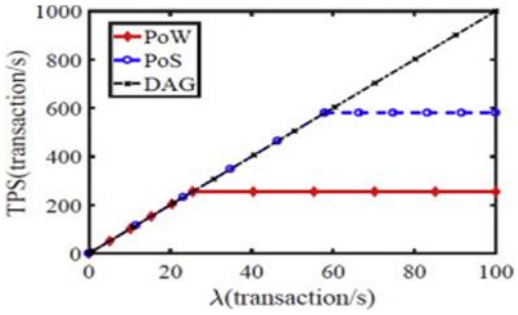


Fig 8 Number of Transactions

7. Limitations and Prospects

Blockchain is a promising technology, but there are still challenges to overcome before widespread adoption. These challenges vary by domain, but can be addressed through ongoing research and development.

7.1 Blockchain for enterprise

Scalability is less of a concern for enterprise blockchain than for public blockchain because participants are already identified. Yet, it's crucial to take into account the usage context and performance metrics in order to optimize variables like transaction throughput, validation latency, energy costs, and storage fees in order to achieve scalability. Initiatives like breaking up a global ledger into smaller sub-ledgers or optimizing storage by adopting a blockchain hierarchy can be implemented to solve scalability. Also, by utilizing strategies like ring signature, zero knowledge proof, and homomorphic encryption, enterprise blockchain can accomplish anonymity.

7.2 Healthcare Industry

The protection of privacy and security in order to safeguard patient medical information presents a special challenge for the healthcare sector. Due to the drawbacks of centralized data storage in medical applications and organizations, interoperability is also a significant issue. The storage of all records in a single database presents challenges for healthcare providers. Data portability and mobility are crucial in the healthcare industry as patients move around more and smart devices and sensors are used more frequently.

7.3 Security Threats

The 51% attack, in which an attacker seizes control of at least 51% of the hash power, is a serious security risk for blockchain networks. The attacker can use a double-spending attack to spend the same cryptocurrency twice by producing a second chain of blocks. The longest chain rule of the blockchain network dictates that if an attacker can convince enough network nodes to follow their chain, it will then take over as the only chain that is valid. While obtaining 51% of the hash power is ideal for a successful attack, a double-spending attack can still be carried out with less than that amount. Nonetheless, the likelihood of success is smaller, and a more robust blockchain network might make such attacks more expensive. Therefore, cryptocurrencies with a high network hash are considered more secure against the 51% attack.

8. Navigating the Blockchain Landscape: A Glimpse into Diverse Frameworks

The blockchain ecosystem thrives on diversity, with a multitude of platforms catering to varied needs and priorities. Let's dive into some prominent players and explore their unique strengths and potential drawbacks:

1. Hyperledger Fabric: Think of it as a modular toolkit for building customized blockchains. Its plug-and-play architecture allows developers to tailor consensus mechanisms, permissioning systems, and privacy features to their specific use cases. While this flexibility empowers niche applications, it can also lead to increased complexity compared to pre-configured platforms.

2. Ethereum: This "global computer" boasts a vibrant developer community and supports a vast array of decentralized applications (dApps). Its smart contract functionality enables automated agreements and intricate interactions, but the public nature and Proof-of-Work consensus mechanism can lead to scalability challenges and high transaction fees.

3. Corda: Designed for the financial sector, Corda prioritizes security and privacy. Its focus on trade finance agreements offers enhanced data control and confidence for sensitive transactions. However, its niche focus may limit its applicability to broader blockchain use cases beyond finance.

4. Quorum: Think of it as a permissioned Ethereum, specifically tuned for enterprise adoption. By eliminating public access and tweaking the consensus mechanism, Quorum enhances transaction speed and reduces energy consumption, making it appealing for private business networks. However, sacrificing the open nature of public blockchains may limit its wider reach and innovation potential.

Beyond the Big Four: This is just a glimpse into the diverse blockchain landscape. Platforms like Hyperledger Sawtooth, Tezos, and Cosmos further expand the spectrum of capabilities and target specific needs. As the technology continues to evolve, new architectures will emerge, addressing current limitations and pushing the boundaries of what's possible.

Each offers unique strengths and weaknesses, making it crucial to carefully analyze your specific needs and choose the framework that best aligns with your project's goals. By understanding the diverse players in this dynamic field, you can navigate the blockchain landscape with informed

decisions and unlock its true potential for your endeavours.

9. Conclusion

Due to its immutable, transparent, and distributed properties, which guarantee that transactions and data stored on it are tamper-proof and can be verified by any node in the network, blockchain technology has recently revolutionised the computing industry. The blockchain's smart contract, which is used in numerous industries, is one of its most intriguing uses. A consensus mechanism is required to add a block to the blockchain; this procedure is sometimes referred to as mining. The background theory of blockchain, its numerous consensus techniques, and their advantages and disadvantages have all been thoroughly examined in this study article. To address some of these challenges, we have proposed a novel consensus mechanism, PoC, that considers reliability, credibility, and efficiency as crucial factors in a blockchain environment. We have also conducted a performance analysis comparing PoC with existing PoW consensus mechanisms. Our future research will focus on the feasibility of implementing PoC in different blockchain platforms. In today's business market, blockchain has become an essential platform with its decentralised and immutable attributes, and consensus plays a vital role in its functioning by facilitating the addition of valid blocks to the blockchain.

Author contributions

Jalpa Khamar has analyzed the data, conducted research, developed methodology and wrote paper. **Hiren Patel** has supervised the data and provided guidance in preparation of manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] G. O. Young, “Synthetic structure of industrial plastics (Book style with [1] N. Satoshi, Bitcoin: A peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf, Accessed on 23rd of January, 2018.

[2] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain, Future Generation Computer Systems, pp. 1-13, 2017.

[3] Z. Hess, Y. Malahov, J. Pettersson, Eternity blockchain: The trustless, decentralised and purely functional oracle machine, White paper, 2017 Available: https://aeternity.com/aeternity-blockchain-whitepaper.pdf, Accessed on 23rd of January, 2018.

[4] A. Ekblad, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data, 2016, White paper, 2016, Available: https://www.media.mit.edu/publications/medrecwhite paper/, Accessed on 23rd of January, 2018.

[5] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: International Conference on Open and Big Data, OBD, pp. 25-30, 2016.

[6] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst., 2016, pp. 218, DOI: https://doi.org/10.1007/s10916-016-0574-6.

[7] SHuckle, R. Bhattacharya, M. White, N. Beloff, Internet of things, blockchain and shared economy applications, Proc. Comput. Sci. 98, pp. 461-466, 2016.

[8] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nano payment scheme for golem, Available: http://golemproject.net/doc/GolemNanopayments.pdf , 2015.

[9] P.Hurich, The virtual is real: An argument for characterising bitcoins as private property, in: Banking & Finance Law Review, vol. 31, Carswell Publishing, 2016.

[10] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing, 2017.

[11] Y. Zhang, J. Wen, The IoT electric business model: Using blockchain technology for the internet of things, Peer-to- Peer Netw. Appl., pp. 1-12, 2016.

[12] J. Sun, J. Yan, K.Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Financ. Innov., 2016, DOI: https://doi.org/10.1186/s40854-016-0040-y.

[13] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016.

[14] E.Nordstr.m, Personal Clouds: Concedo (Master’s thesis), Lulea University of Technology, 2015.

[15] J.S.Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015.

[16] M. Correia, G. S. Veronese, N. F. Neves, and P.

Verissimo, Byzantine consensus in asynchronous message-passing systems: a survey, International Journal of Critical Computer-Based Systems, vol. 2, no. 2, pp. 141–161, 2011.

[17] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, Consensus in the Age of Blockchains, Available: https://arxiv.org/pdf/1711.03936.pdf, Accessed on 23rd of January, 2018,

[18] Y. Li, Z. Luo, J. Yin, L. D. Xu, Y. Yin, Z. Wu, Enterprise pattern: integrating the business process into a unified enterprise model of modern service company, vol. 11, no. 1, 2015, DOI: https://doi.org/10.1080/17517575.2015.1053415.

[19] A.Meidan, J. A. Garcia-Garcia, M. J. Escalona, I. Ramos, A survey on business processes management suites, Computer Standards & Interfaces, vol. 51, pp. 71-86, 2017.

[20] H.Ariouat, C. Hanachi, E. Andonoff, F. Benaben, A conceptual framework for social business process management, Procedia Computer Science, vol. 112, pp. 703-712, 2017.

[21] F. Rahimi, C. Moller, L. Hvam, Business process management and IT management: the missing integration, International Journal of Information Management, vo. 36, no. 1, pp. 142-154, 2016.

[22] G. Bracha, S. Toueg, Asynchronous consensus and broadcast protocols, Journal of the ACM (JACM), vol.32 no.4, pp.824-840, Oct. 1985.

[23] M. Castro, B. Liskov, Practical Byzantine Fault Tolerance, in the Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999.

[24] 19 Industries The Blockchain Will Disrupt [Online], Available:http://futurethinkers.org/industries-blockchaindisrupt/, Accessed on 5th of February, 2018.

[25] C. Hammerschmidt, Consensus in Blockchain Systems. In Short, Available:https://medium.com/@chrshmmmr/consensus-in-blockchain- systems-in-short-691fc7d1fefe, Accessed on 5th of February, 2018.

[26] A. Baliga, Understanding Blockchain Consensus Models, Whitepaper, 2017.

[27] M.Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, In Proc. IFIP WG 11.4 Workshop Open Res. Problems Netw. Secure. (iNetSec), pp. 112-125, 2015,

[28] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, July 1982

[29] Fedor Muratov, Andrei Lebedev, Nikolai Iushkevich, Bulat Nasrulin,Makoto Takemiya Soramitsu, “YAC: BFT Consensus Algorithm for Blockchain”, arXiv:1809.00554v1 [cs. DC] 3 Sep 2018

[30] Siamak Solat “RDV: An Alternative to Proof-of-Work and a real Decentralized Consensus for Blockchain”,ACM ISBN 978-1-4503-6050-0/18/11http://doi.org/10.1145/3282278.3282283

[31] Tae Kim, Jungha Jin, Keecheon Kim ,”A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority)”, 978-1-5386-5041-7/18/ ©2018 IEEE,http://doi.org/10.1145/3282278.3282283

[32] Sungmin Kim, Joongheon Kim “POSTER: Mining with proof of probability in blockchain”, ACM ISBN 978-1-4503-5576-6/18/06, http://doi.org/10.1145/3196494.320192

[33] Phil Daian, Rafael Pass, Elaine Shi, "Snow white: Provably secure proofs of stake", Cryptology ePrint Archive Report 2016/919, 2016.

[34] Rafael Pass and Elaine Shi. 2017. The Sleepy Model of Consensus. In ASIACRYPT 2017, Part II (LNCS), Tsuyoshi Takagi and Thomas Peyrin (Eds.),Vol. 10625. Springer, Heidelberg, 380–409

[35] Badertscher, C., Gazi, P., Kiayias, A., Russell, A., & Zikas, V. (2018). Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability. ACM Conference on Computer and Communications Security

[36] khamar, J., Patel, H. (2021). An Extensive Survey on Consensus Mechanisms for Blockchain Technology. In: Kotecha, K., Piuri, V., Shah, H., Patel, R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore.https://doi.org/10.1007/978-981-15-4474-3_40

[37] De Angelis, Stefano. (2018). Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains.

[38] Bach, L. M., Branko Mihaljevic, and Mario Zagar. "Comparative analysis of Blockchain consensus algorithms." 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018.

[39] Yuan, Yong, and Fei-Yue Wang. "Towards

Blockchain-based intelligent transportation systems." 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016.

[40] J. Ray, "Proof of stake FAQ", https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, 2018.

[41] Nguyen, Giang-Truong, and Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain." Journal of Information processing systems 14.1 (2018).

[42] Bentov, I., et al. "Proof of activity: extending bitcoin's proof of work via proof of stake. ACM SIGMETRICS Perform." Eval. Rev 42.3 (2014): 34-37.

[43] Milutinovic, Mitar, et al. "Proof of luck: An efficient Blockchain consensus protocol." proceedings of the 1st Workshop on System Software for Trusted Execution. ACM, 2016.

[44] Salimitari, Mehrdad, and Mainak Chatterjee. "An overview of blockchain and consensus protocols for IoT networks." arXiv preprint arXiv:1809.05613 (2018).

[45] Huang, Dongyan, Xiaoli Ma, and Shengli Zhang. "Performance analysis of the Raft consensus algorithm for private blockchains." IEEE Transactions on Systems, Man, and Cybernetics: Systems (2019).

[46] Miguel Castro and Barbara Liskov." Practical Byzantine Fault Tolerance". http://pmg.csail.mit.edu/papers/osdi99.pdf, 1999

[47] De Angelis, Stefano, et al. "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain." (2018).

[48] NEO White paper (2014). Availablehttp://docs.neo.org/en-us [Accessed: 10 FEB 2018.

[49] Stuart Haber, W. Scott Stornetta: How to Time-stamp a Digital Document. In: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, pp.437-455, (August 11-15) (1990)

[50] S. Nakamoto: Bitcoin A Peer-to-Peer Electronic Cash System.https://bitcoin.org/bitcoin.pdf(2008.)

[51] Petri Helo, Yuqiuge Hao: Blockchains in operations and supply chains: A model and reference implementation. Computers & Industrial Engineering, Volume 136, pp. 242-251, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2019.07.023.(http://www.sciencedirect.com/science/article/pii/S0360835219304152)(2019)

[52] A. Litke, D. Anagnostopoulos, and T. Varvarigou: Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. Logistics, vol. 3, no. 1, p. 5, (2019)

[53] M. Kouhizadeh and J. Sarkis: Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability, vol. 10, no. 10, p. 3652(2018)

[54] G. Danezis and S. Meiklejohn: Centrally Banked Cryptocurrencies (2015)

[55] K. Biswas and V. Muthukkumarasamy: Securing smart cities using Blockchain technology. In: 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS, pp. 1392-1393, (December 12, 14) (2016)

[56] P. T. S. Liu: Medical record system using Blockchain, big data and tokenization. In: 18th International Conference on Information and Communications Security, pp. 254-261 ICICS (November 29- December 2 (2016)

[57] M. Vukoli: The quest for scalable Blockchain fabric: Proof-of-work vs. BFT replication. In: IFIP WG 11.4 International Workshop on Open Problems in Network Security, pp. 112-125. iNetS (2016)

[58] F. Idelberger, G. Governatori, R. Riveter, and G. Sartor: Evaluation of Logic-Based Smart Contracts for Blockchain Systems. Cham, Switzerland, pp. 167-83(2016)

[59] D. Kraft: Difficulty control for Blockchain-based consensus systems. Peer-to-Peer Networking and Applications, vol. 9, pp. 397-413, (201601-01) (2016)

[60] Tama, Bayu Adhi, et al: A critical review of blockchain and its current applications. In: International Conference on Electrical Engineering and Computer Science (ICECOS), IEEE (2017)

[61] Drescher, Daniel: Blockchain basics. Berkeley, CA: Apress (2017)

[62] M. Swan. Blockchain: Blueprint for a New Economy. O'Reilly, US (2015)

[63] Schwartz, D., Youngs, N., & Britto, A: The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5, 8(2014)

[64] Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M: Corda: an introduction. R3 CEV, August, 1, 15(2016)

[65] Sousa, J., Bessani, A., &Vukolic, M: A byzantine fault-tolerant ordering service for the hyper ledger fabric Blockchain platform. In: 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN) (pp. 51-58). IEEE. (June) (2018)

[66] Baliga, A: Understanding Blockchain consensus models. In: Persistent (2017)

[67] Guo, Y., & Liang, C: Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24(2016)

[68] De Angelis, Stefano: Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains (2018)

[69] L. Lamport, R. Shostak and M. Pease: The Byzantine Generals Problem. In: Acm Transactions on Programming Languages & Systems, vol. 4, pp. 382-401(1982)

[70] Bach, L. M., Branko Mihaljevic, and Mario Zagar: Comparative analysis of Blockchain consensus algorithms. In: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE (2018)