STM JOURNALS

E-Commerce for Future & Trends

ISSN: 2454-9347
Volume 9, Issue 1, 2022
DOI (Journal): 10.37591/ECFT

http://computers.stmjournals.com/index.php?journal=ECFT&page=index

Research ECFT

Proof-of-Minimum Privacy Leak Consensus Strategy in Blockchain

Manas Kumar Yogi*, Yamuna Mundru, Siva Satya Prasad Pennada

Abstract

In this study, we propose a novel consensus algorithm to preserve the security and privacy of a transaction. We propose a Proof-of-Minimum Privacy Leak consensus strategy. This means that the competing nodes which participate in the competition to mine the next block should give a proof of minimum privacy leak during its transaction. Only this proof will give highest votes to that node, and it will be elected as the leader. The minimum privacy leak of a node participating in a Blockchain depends on various factors intrinsic to the Blockchain application. For example, if the application is related to healthcare, it will be related to the sensitive data of a patient, if it is a banking application, it will be related to monetary aspects of the account holder, etc. For our study, we apply the proposed approach to a smart voting system where Blockchain is deployed. Here, the participants' details during voting are private data and there are provisions to reduce the voter privacy so that the participants of the smart voting system gain trust in the system rather than doubting that their privacy will be preserved or not. Our proposed mechanism performs better than recent popular consensus algorithms as shown in the experimental result. The results are displayed in terms of improved scalability, reliability and degree of increased trust.

Keywords: Blockchain, consensus, ledger, distributed, privacy

INTRODUCTION

A consensus protocol is an instrument that permits clients or machines to organize in a dispersed setting. Its necessities to guarantee that all specialists in the framework can settle on a solitary wellspring of truth, regardless of whether a few specialists' fizzle. All in all, the framework should be fault tolerant. In a unified arrangement, a solitary element has control over the framework [1]. Most of the time, they can make changes, however, there is no intricate management framework for reaching consensus among numerous heads. In any case, in a decentralized arrangement, it is a completely separate story. Let us assume that we are working with a dispersed data set, how would we agree on what sections get added? Conquering this test in an environment where outsiders have little to no trust in one another was possibly the most important improvement preparation for Blockchain. In this study, we will look at how consensus calculations are essential to the operation of digital forms of money and transmitted records. Instruments for accomplishing consensus are essential to the working of circulated frameworks. Many accept that the best advancement in Bitcoin was the utilization of Proof of Work to empower clients to settle on a common arrangement of realities [2]. Consensus calculations today support advanced cash frameworks, however Blockchain permits designers to run code across a disseminated network. They are presently a foundation of Blockchain innovation and are basic to the drawn-out feasibility of the different organizations in existence. Before we continue on to the consensus conventions, let us analyze a factual reality connected with consensus conventions. Hypothetically, the Blockchain is viewed as compromised, assuming that a programmer gains

***Author for Correspondence**
Manas Kumar Yogi

Assistant Professor, Department of Computer Science & Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

Received Date: April 12, 2022
Accepted Date: April 25, 2022
Published Date: April 29, 2022

Citation: Manas Kumar Yogi, Yamuna Mundru, Siva Satya Prasad Pennada. Proof-of-Minimum Privacy Leak Consensus Strategy in Blockchain. E-Commerce for Future & Trends. 2022; 9(1): 24–35p.

admittance to 51% or a more critical piece of the organization [3]. The different sorts of consensus conventions tackle the 51% assault issue in different ways.

TARGETS OF BLOCKCHAIN CONSENSUS MECHANISM

Unified Agreement

One of the great goals of consensus systems is accomplishing unified agreement. In contrast to incorporated frameworks where having a trust on power is fundamental, clients can work even without building trust in one another in a decentralized way [4]. The conventions implanted in the distributed Blockchain network guarantees that the information associated with the interaction is valid and exact, and the situation with the public record is cutting edge.

Adjust Economic Incentive

With regards to building a trust-less framework that controls all alone, adjusting the interests of members in the organization is an unquestionable requirement. A consensus Blockchain convention, in the present circumstance, offers compensations for appropriate conduct and rebuffs the agitators [5]. Thusly, it guarantees controlling monetary motivators as well.

Fair and Equitable

Consensus instruments empower anybody to take part in the organization and utilize similar rudiments. Thusly, it legitimizes the open-source and decentralization property of the Blockchain framework [6].

Prevents Double Spending

Consensus instruments chips away at the premise of specific calculations to ensure that the main exchanges are remembered for the public straightforward record that are checked and is significant.. This tackles the customary issue of twofold spending, i.e., the issue of expenditure of computerized money two times.

Fault Tolerant

One more attribute of the Consensus technique is that it guarantees that the Blockchain is fault-tolerant, steady, and solid. This implies, the administered framework would work endless times even on account of disappointments and dangers.

RELATED WORK

This segment examines the beautiful arrangement calculations in Blockchain that are of late proposed. The investigation works that have performed relative examination of understanding calculations in Blockchain are likewise explored.

Secure Sharding

ELASTICO is proposed as an adaptable arrangement calculation for authorization less Blockchain. Conversion standard scales straightforwardly with the computation related with mining strategy. That is, with farther computation power, farther trade blocks are reused. This estimation can suffer with adversaries that hold one fourth of indisputably the computational power [7]. The guideline believed is to segment an association into little pieces known as sheets. Each commission processes a disjoint approach of game-plans and entire system is parallelized. This calculation is not quite the same as the old-style complex calculation in a manner the understanding condition is executed in probabilistic way. Each fair interaction coordinates its concurred esteem with a requirement capacity and really looks at its legitimacy. The outcome is acknowledged provided that it fulfils the requirement of the work. All boards play out a traditional complicated understanding. The last commission consolidates the outcomes (shards), all things considered. Some security packages are characterized, and calculation is approved regarding every one of these bundles that features its security strength.

Starters are run on Amazon EC2 including up to 1600 thumps. Worried of this computation, new guideline is added to the publically open guideline for Bitcoin.

SCP: A Computationally Versatile Byzantine Agreement Calculation for Blockchain

SCP is proposed as a new computationally flexible Blockchain game plan estimation based on Convoluted Graphs. Computationally adaptable means the calculation is adequately adaptable to change the data transmission utilization by adjusting the computational boundaries practically equivalent to as position of trouble in validation of work (PoW) medium [8]. If we increase the computational power, similarly an addition in expansion will be normal.

In SCP, diggers with less computational capacity are allowed to come in for a commission and be remembered for the popularity-based link. Additionally, bargains are separated marginally among the information blocks acting in decentralization of organization. No focal instrument is requested, consequently excepting the difficulty of weak link.

The SCP calculation is conspired to adaptable digital currency SCoin. Additionally, Merkel tree is utilized that tries not to twofold spend issue. Twofold spending is forestalled locally by checking on the off chance that an exchange has just a single issue or not [9]. SCP is demonstrated to check directly with the increment in computational limit without adding the data transfer capacity in a quadratic way.

Leader-free Byzantine Consensus Algorithm

Many-sided predicated arrangement issue is mooted for a mostly coterminous framework. A halfway coterminous framework is an offbeat framework that comes to coterminous mode in the end. Planning a deterministic pioneer free calculation for a mostly coterminous framework is a difficult errand. A trailblazer free estimation really contains adjusts in which all correspondence happens among the thumps [10]. This study proposed a pioneer free calculation to accomplish arrangement in incomplete coterminous framework. The arrangement chief free calculation for coterminous framework is reached out for halfway coterminous framework. The understanding calculation considered in this study for coterminous frameworks is predicated on intelligent consistence issue. Each interaction figures a bunch of values with each worth addressing a component for a cycle. The right cycles think of similar arrangement of values [11]. This calculation is stretched out in two ways: One is by utilizing parameterized understanding calculation in which various models of shortcoming are permitted in arrangement.

On the Security and Performance of Proof of Work Blockchain

Quantitative packing is used to evaluate security and execution of PoW game plan predicated Blockchain in regards to various associations and getting related limits. PoW understanding is embraced by outrageous of the being Blockchain. The varieties of PoW positively stand apart to the point of being seen recorded as a hard copy concerning security assessment [12].

Blockchain Consensus: An analysis of Proof-of-Work and its applications

As the issue intricacy is expanded, digging time for new squares is likewise expanded. Different tasks of Blockchain overall are additionally surveyed. PoW is a significantly involved understanding medium in Blockchain results.

It was first presented by Bitcoin. In this calculation, every one of the knocks vote by working a validation of work and produce new squares with their own calculation power [13]. Assuming this happens, additionally comparable a bunch can handle the entire framework by developing a longest chain. To ensure a comprehension among taking an interest thump of an association, a popularity based medium is mentioned. In Nakamoto game-plan, a group that scores a sweepstakes is named as a pioneer. In bitcoin, first bunch to break bewilderment walks away with a sweepstakes. Customary

intricate shortcoming patience (BFT) calculations are likewise used to accomplish arrangement among the knocks including expressly propelling medium.

The Blockchain Consensus Layer and BFT

In this study, the creators concentrated on the association of complex issue avoidance calculations and Blockchain calculations. A layered perspective on Blockchain is introduced that features its different elements. Mutt influence including Nakamoto calculation and BFT is additionally mooted [14].

(Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchain

Arrangement estimation without imprint, trailblazer, and randomization is presented. The calculation reduces the multi respected based Byzantine agreement issue to twofold Byzantine plan issue. Matched events of understanding are run in equivalent by which a value is picked in steady time [15]. The optimality of proposed arrangement is represented speculatively by multiple researchers in recent developments.

Implicit Consensus: Blockchain with Unbounded Through-put

An irrefutable agreement model is proposed in which each bundle has its individual Blockchain. Fundamental benefit procured with this is an unbounded increase. End property of BFT is dislodged with a property of tone-interest. Understanding is not ensured for each exchange. This makes this plot adaptable with direct correspondence multifaceted nature. Rather of comprehension of trade obstructs, an outstanding sort of squares are considered, known as assigned spot blocks. The show and alternate points of view are taken apart speculatively.

Design and Implementation of a Proof-of-Stake Consensus Algorithm for Blockchain

This disquisition work discusses the introduction of approval of stake (PoS) game plan estimation in Blockchain. PoW is one of the emphatically mooted bits of Bitcoin. It is utilized as a method for managing closing a square endorser predicated on the computational difficulty of excavators in discovering complex fine issue [16]. Another square underwriter is labelled utilizing an inconsistent model predicated on how much stake that an excavator holds. With this, the power burden in booby-entangling a square will get generally diminished when stood out from creature power like estimation in PoW. Ouroboros and Casper are the two striking PoS predicated plan shows. Ouroboros picks the accomplice inconsistently by a safeguarded coin flipping estimation and an effective time places combination. Casper gives a more weak affirmation as for how critical stake is obliged by enemy to create disrupting impact.

PPCoin: Peer-to-Peer Crypto-Currency with Proof-of- Stake

This study reviews endorsement of-stake calculation that confines the energy utilization as it impacts the security of a Blockchain network. Plan of a distributed digital money PPcoin is presented that has no reliance on energy utilization. The plan of a validation of stake calculations is mooted concerning the consensus of coin age. Coin age is the timeframe for which a money sum is held [17]. Dissimilar to PoW, maker of another square is labelled deterministically relying upon its abundance (Stake).

A Proof-of-Trust Consensus algorithm for Enhancing Accountability in Crowdsourcing Services

A game plan computation is proposed for openly supporting organizations. Deals validators are named predicated on the trust potential gains of thumps. Two estimations, Shamirs secret sharing computation and RAFT pioneer political race are used in its arrangement. The flexibility challenges related with the standard BFT computations are tended to the comprehension estimation are divided into four phases [18]. Logically, work 1 is centered around pioneer political race in association using Raft pioneer political race computation. Next stage picks exchange validators utilizing projecting a

surveying structure medium. In stage 3, social event of bangs (that are named for exchange proof past stage) support the game-plans. Last stage collects the upheld strategies and affiliate it with the Blockchain.

RMBC: Randomized Mesh Blockchain Using DBFT Consensus Algorithm

Assortment of evaluation predicated BFT game plan estimation is proposed and mooted. This computation generally settled the two issues in PoW and BFT estimations autonomously. In PoW, there is an expense departure with BFT as number of shocking certified factors in an affiliation increments by a gigantic number besides invalid strategies cannot be foiled. There are two layers in plan getting cycle [19]. The essential stage incorporates a BFT estimation. Substitute stage performs social occasion of related divisions. From there on out, a verifier is marked from each office. Trade is supported if the first and substitute arrangement stage are indistinct.

PoPF: A Consensus Algorithm for JCLedger

Formulators can change the pall express associations utilizing a model known as JointCloud. JCLedger is a Blockchain predicated result for JointCloud. The contenders for mining are named using two factors figure paid by party and number of times the party displayed as accountant. The makers have likely evaluated the estimation through amusement concerning movement of accountants. The delicacy and execution related viewpoints are not related with primers [20].

CONSENSUS IN DISTRIBUTED SYSTEMS AND BLOCKCHAIN

Understanding is a centre distortion in given structures and not restricted to Blockchain. It applies to scripts in which different cycles or pounds need to keep an ordinary condition of information thing. Endorsement less and permissioned Blockchain are two basic kinds of Blockchain. In consent less Blockchain, pounds are dark. One more modified trade square can be added acting in a fork. Fork happens where a significant trade confuses with the invalid bone [21]. The essential thing of arrangement calculation is to accomplish understanding among the knocks, comparable to that each bunch settles on one genuine worth.

Agreement is as yet critical to accomplish all things considered as the knocks are not secure. Figure 1 portrays the armature of Blockchain. By and large, arrangement is worth to consider where the bangs of an affiliation are flawed, or they convey in a touchy manner. Arrangement is achieved in appropriated structures as for specific dissatisfactions [22]. Further, while describing understanding structure correspondence model similar as coetaneous or odd is furthermore remembered to be material. There are lovely requests of dissatisfactions crash frustration, streak disillusionment, elision frustration, security frustration, programming disillusionment, disperse frustration, transient disillusionment, and biological anxiety [23].

Continuous from this, each computation is also flowed predicated on correspondence model tantamount to as coterminous, inadequate coetaneous, and strange. Randomized getting gives affirmation to game-plan, credibility, and end conveys with some likelihood respect [24]. Tolerating no likelihood is associated, additionally the outcomes are applied to as deterministic. Monte Carlo understanding works by running Monte Carlo assessment on each correspondence or load with unequivocal ran information. Values from different cycles are joined to a by and large getting worth. Another requesting is Las Vegas, where each arranging round has a chance. There are also live trailblazer-based plan estimations where a trailblazer is indicated to pick an end on comprehension. Trailblazer free comprehension computations are furthermore proposed. Figure 2 portrays the overall design and arrangement of understanding instruments in circulated frameworks.

PROPOSED MECHANISM

We propose a setup of the Blockchain system where instead of selecting a node randomly, the election algorithm allows all the participating nodes to claim their stake to mine the next block based on a certain characteristic. This characteristic is the minimum privacy leak. We advocate a factor

called as Privacy Sensitivity factor, PSF for each node. The value of PSF for all the nodes are pooled into a decision-making application, which compares respective PSF values of all the nodes and the node having the minimum PSF value is given chance to mine the next block. The overall illustration is shown in Figure 3 below.

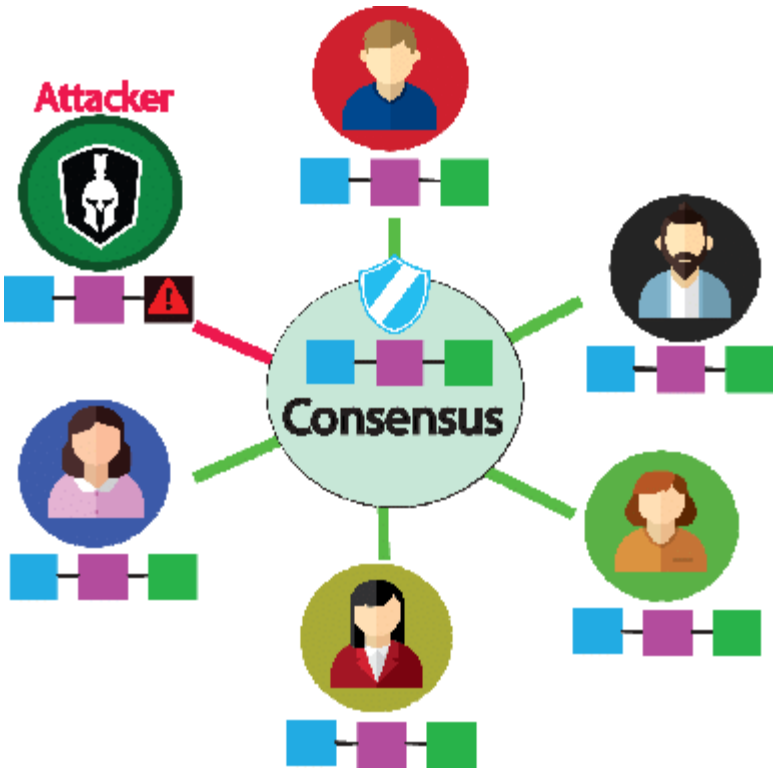

Figure 1. Consensus in distributed environment.

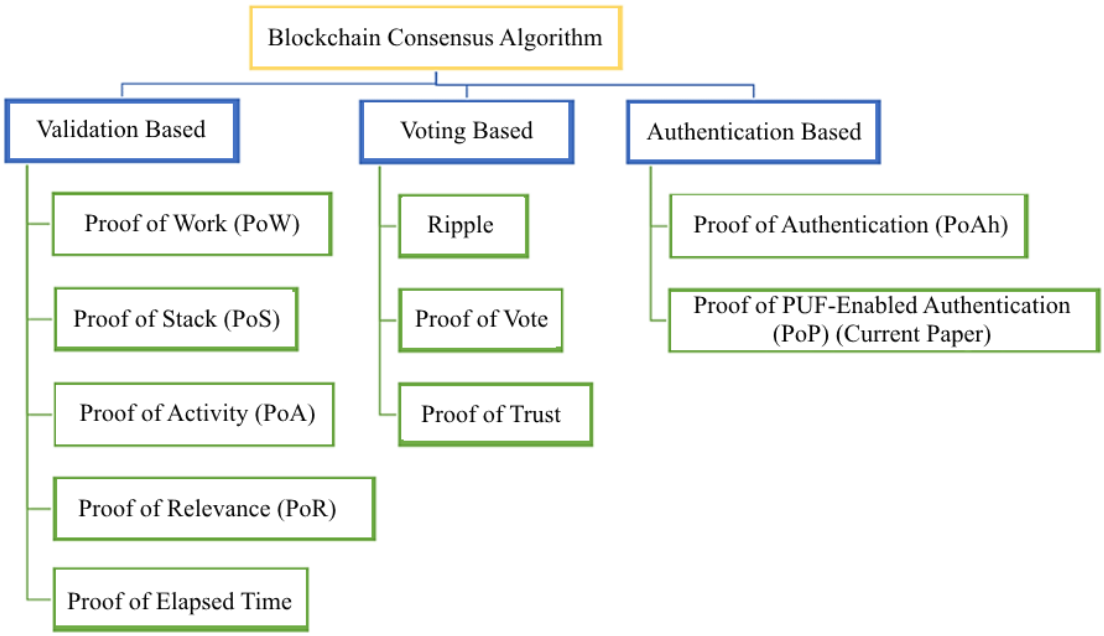

Figure 2. Categorization of consensus algorithms.

The node which has the minimum privacy leak is called as Privacy Deprecator (PD), instead of a miner which is the term used in Proof-of-work consensus mechanism.

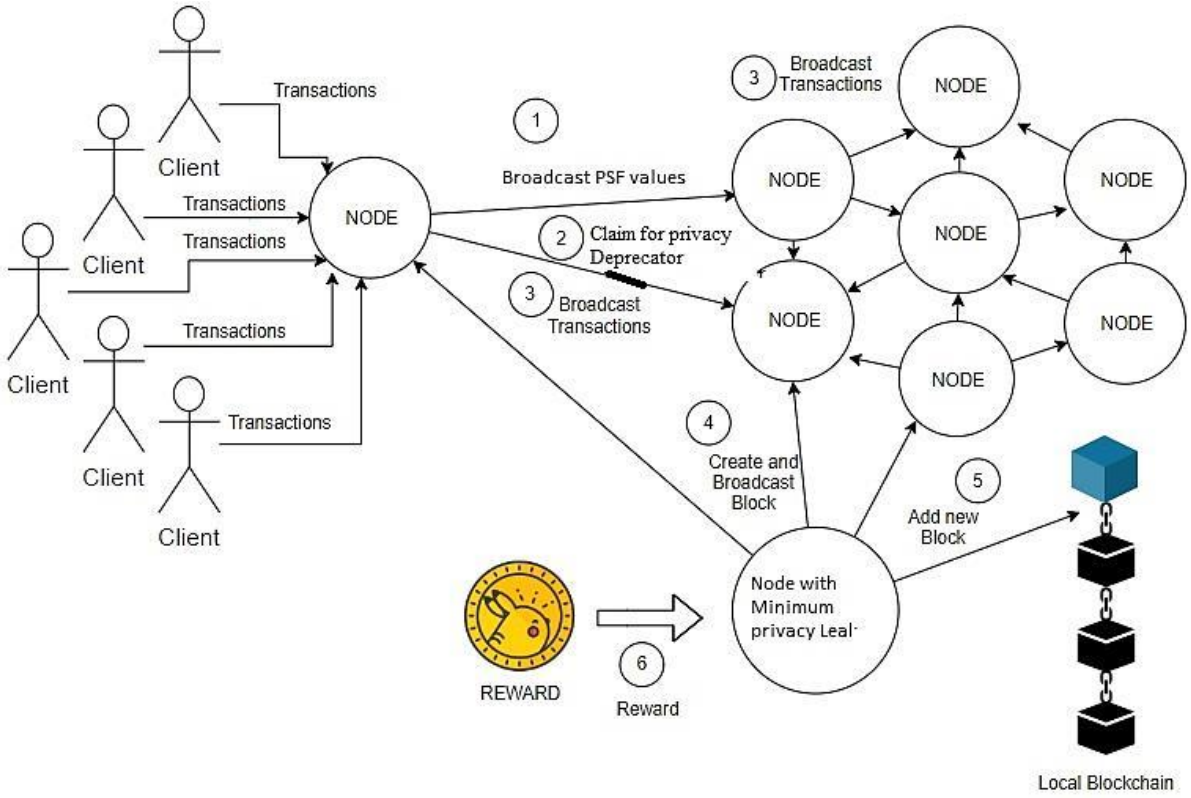

Figure 3. Illustration of Proof-of minimum privacy leak mechanism.

Flow of Proposed Approach

- *Step 1:* A specific node computes internally a privacy sensitivity value (PSF) and broadcasts it to all the other nodes. This is for enhanced transparency.
- *Step 2:* Through its PSF value, it claims to become the privacy Deprecator for the whole network. But the node has to wait till the consensus is reached among all the nodes in the network.
- *Step 3:* The transaction is broadcast into the network of nodes by the node which claims to be the privacy deprecator.
- *Step 4:* The node which has become the privacy deprecator gets the chance to mine the next block.
- *Step 5:* The new block mined successfully by the Privacy deprecator node is added into the new Blockchain.
- *Step 6:* The node which is now the Privacy deprecator gets a reward in the form of a transaction fees.

In most of the current methods of consensus algorithms, all nodes have equal chances of getting elected as a master node to get the chance for mining the next bock. But if a malicious or compromised node becomes the master then it will cause havoc on the Blockchain. To avoid such mishaps, in our novel approach, the nodes which cannot provide a proof of privacy leak of the transactions, must not enter into a cycle in which they can claim to be a privacy deprecator.

This prohibition allows nodes with proof of privacy leaks only to be in a competition to become the next master. The main benefit of this method is that power consumption of the Blockchain network is reduced significantly. Also, the user gains trust in the Blockchain network as they are assured of minimum privacy leak during performing transactions frequently over a considerable period of time. Many researchers have proposed hybrid consensus algorithms with low latency and

throughput but designing such complex consensus techniques has been a continuous challenge and so our proposed approach is designed with less complexity taken only the privacy sensitivity value (PSF) as metric to rule the Blockchain network. During execution of smart contracts, our proposed mechanism is quite scalable in nature.

We advocate the concept of prominence value to evaluate the node's proof of minimum privacy, we then utilize its value to infer the node's creditability and reliability value, and then the consensus node is hierarchically placed to be the next privacy deprecator node based on the prominence value to reduce network communication between nodes. The prominence value is calculated as follows:

$$PV_{n+1}=PV_n+\min \{PSF_1, PSF_2, ..PSF_n\} \quad (1)$$

In the above Eq. (1), PV denotes prominence value of a node n and PSF denotes the privacy sensitivity value.

So, the node which acts as the first privacy deprecator gives proof of minimum privacy and the next node which claims to be the privacy deprecator should provide the next proof of minimum privacy leak.

EXPERIMENTAL RESULTS

We have considered November Top 10 crypto performance dataset from Kaggle. This dataset has a total of 76 crypto currencies data values for 1 month. We have applied our proposed approach and found the transaction speed as tabulated below for the top 10 crypto currencies as shown in Table 1.

Table 1. Top 10 crypto performance dataset.

S. No.	Name of the Crypto currency	Transactions Per second
1	Binance Coin	187
2	Bitcoin	45
3	Cardano	541
4	Dogecoin	629
5	Ethereum	98
6	Polkadot	122
7	Solana	823
8	Tether	80
9	USD coin	325
10	XRP	467

We can observe from Figure 4 that our novel approach performs relatively better when compared to current popular methods like Proof of stake, Practical Byzantine Fault tolerant algorithm and Proof of work mechanisms. From the graph we can observe that as the degree of private data release increases the percentage increase in performance also increases. This is due to the reason that the deprecator node now gives chance to the next node which claims to release privacy at a minimum level to become the new deprecator node. As the value of degree of private data release reaches one, we can infer that the performance of our proposed algorithm enhances by nearly 8%.

From Figure 5 we can observe that our novel mechanism needs less than 6 messages to pass the information regarding the consensus for the node which claims to be the privacy deprecator and proof of work consensus algorithm needs the maximum messages i.e., around 7 messages to reach the network consensus. Hence, we can say that in terms of reducing the network latency, our proposed approach edges out the other popular methods.

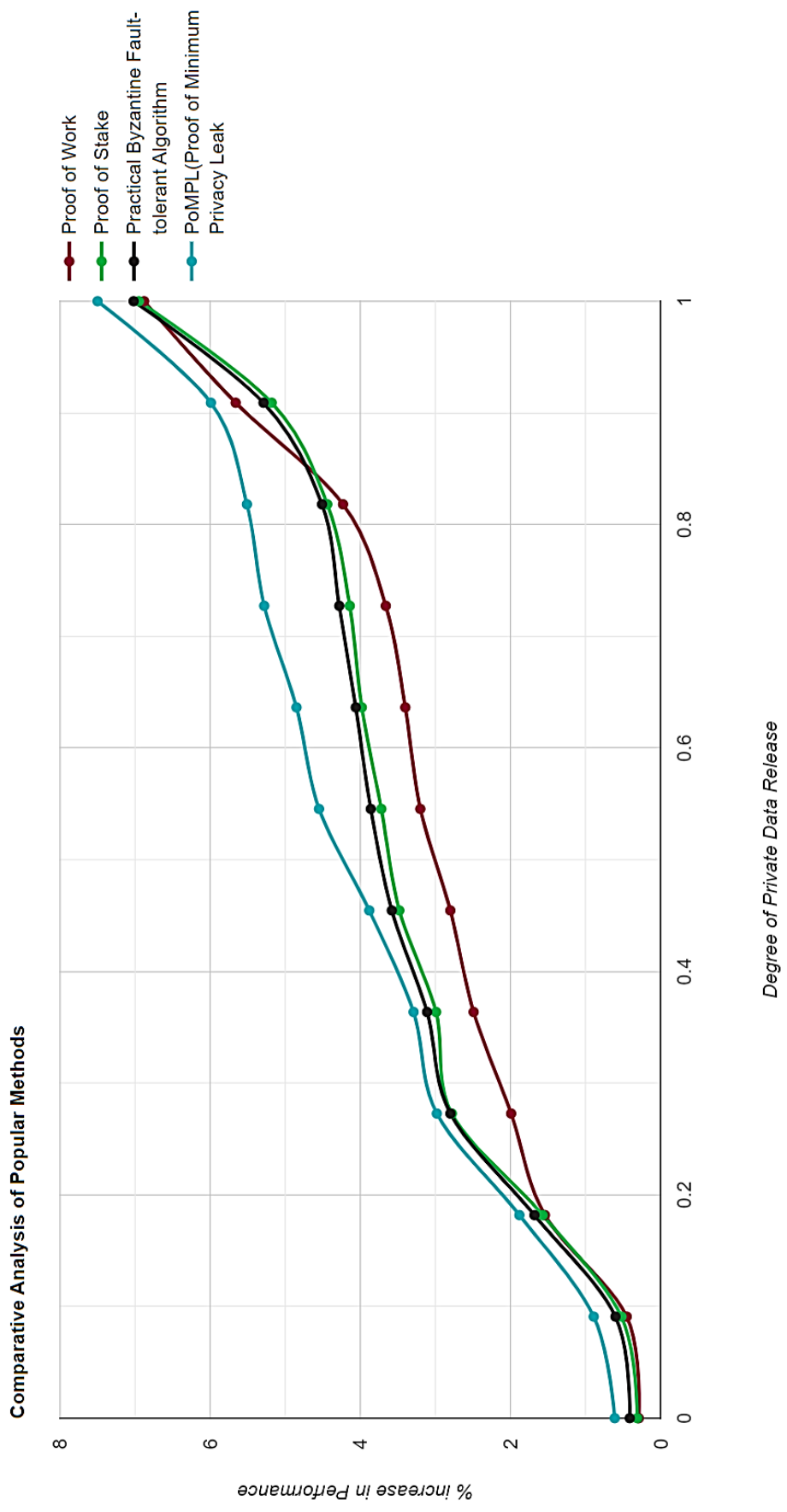

Figure 4. Comparative analysis of popular consensus algorithms.

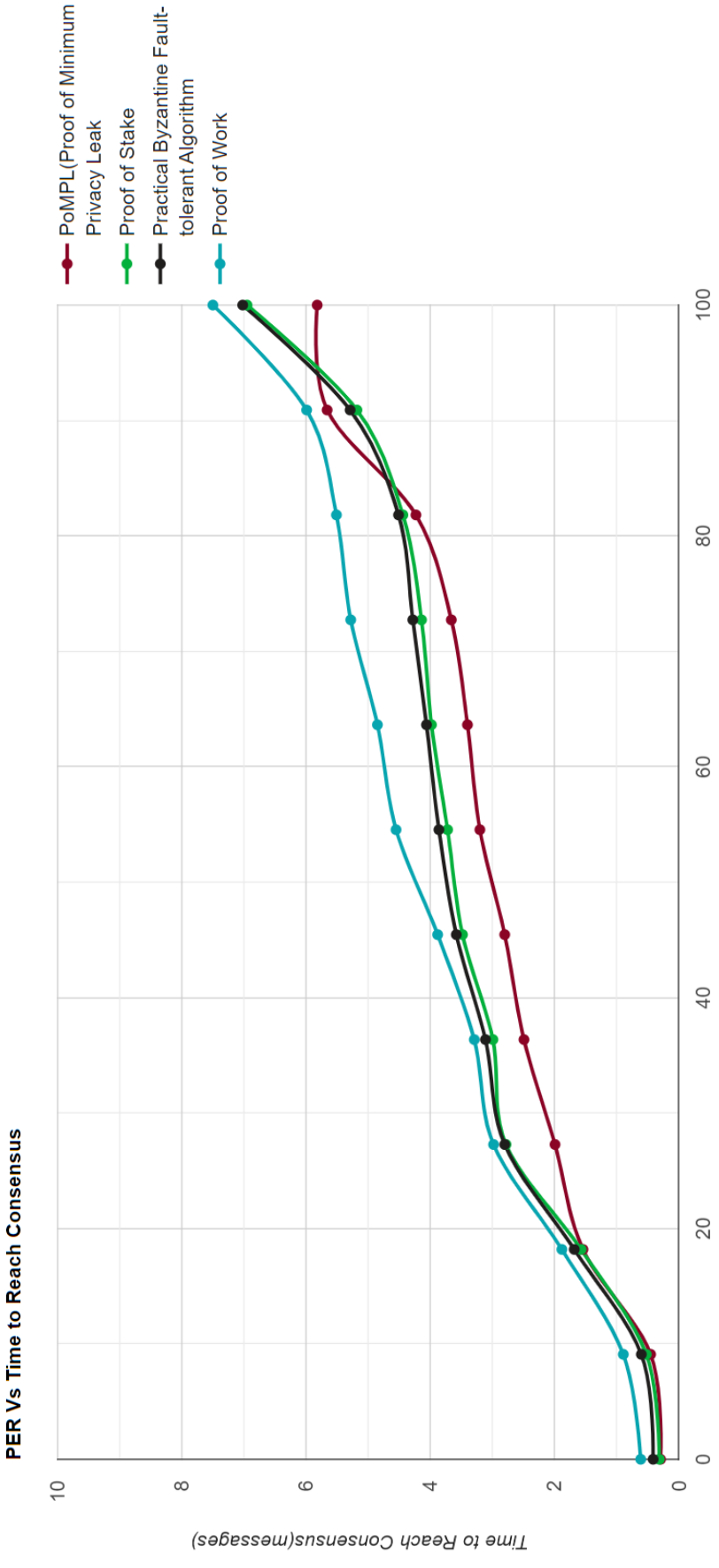

Figure 5. Packet error rate (%) vs. time to reach consensus.

CONCLUSION

Construction of high degree of throughput and reduced latency consensus algorithm which is amicable for multiple node Blockchain network is the main goal of upcoming research work. In future, many improvements in the consensus algorithm will be providing a new direction in this aspect. Our study attempts a privacy-based consensus algorithm where the opportunity of becoming a master in the network should be assigned to a robust node. The robust node is the node which can maintain privacy leak of the transaction at a minimum value. Our approach shows appreciable performance during the experiments against popular consensus algorithm. In future, we want to fuse the differential privacy approach into our current mechanism so that the privacy leak of the transaction is reduced even further.

REFERENCES

1. Weide Cai, Lian Yu, Rong Wang, Na Liu, Enyan Deng. Research on application system development method based on Blockchain. J Softw. 2017; 28(06): 1474–1487.
2. Wang W, Hoang DT, Xiong Z, *et al*. A survey on consensus mechanisms and mining management in Blockchain networks. IEEE Access. 2019; 7: 22328–22370.
3. Pilkington M. Blockchain Technology: Principles and Applications. NY, USA: Social Science Electronic Publishing; 2016.
4. Qifeng Shao, Cheqing Jin, Zhao Zhang, Weining Qian, Aoying Zhou. Blockchain: Architecture and Research Progress. Journal of Computer Science. 2018.
5. Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: A distributed solution to automotive security and privacy. IEEE Commun Mag. 2017; 55(12): 119–125.
6. Sankar LS, Sindhu M, Sethumadhavan M. Survey of consensus protocols on Blockchain applications. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore. 2017; 1–5.
7. Rihong Wang, Lifeng Zhang, Quanqing Xu, Hang Zhou. A Byzantine fault-tolerant consensus algorithm that can be applied to alliance chains. Computer Application Research. 2020; 1–6.
8. Zhao W. Application-Aware Byzantine Fault Tolerance. 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, Dalian. 2014; 45–50. doi: 10.1109/DASC.2014.17.
9. Veronese GS, Correia M, Bessani AN, Lung LC, Verissimo P. Efficient Byzantine Fault-Tolerance. IEEE Trans Comput. 2013 Jan; 62(1): 16–30. doi: 10.1109/TC.2011.221.
10. Bracha G, Toueg S. Asynchronous Consensus and Broadcast Protocols. J ACM. 1985 Oct; 32(4): 824–840.
11. Castro M, Liskov B. Practical Byzantine fault tolerance. Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI), New Orleans, USA. 1999 Feb; 173–186.
12. Gervais A, *et al*. On the Security and Performance of Proof of Work Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria. 2016 Oct 24–28; 3–16.
13. Hou R, *et al*. Research on secure transmission and storage of energy IoT information based on Blockchain. Peer Netw Appl. 2020; 13(11): 1225–1235.
14. Abuidris Y, Kumar R, Yang T, Onginjo J. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI J. 2021; 43(2): 357–370.
15. Gorog C, Boult TE. Blockchain Synchronous Trust Consensus Model. arXiv preprint arXiv:2112.03692. 2021.
16. Khan D, Jung LT, Hashmani MA. Systematic Literature Review of Challenges in Blockchain Scalability. Appl Sci. 2021; 11(20): 9372.
17. Jiang N, Bai F, Huang L, An Z, Shen T. Reputation-Driven Dynamic Node Consensus and Reliability Sharding Model in IoT Blockchain. Algorithms. 2022; 15(2): 28.
18. Joshi S. Feasibility of Proof of Authority as a Consensus Protocol Model. arXiv preprint arXiv:2109.02480. 2021.

19. Kudva S, Badsha S, Sengupta S, Khalil I, Zomaya A. Towards secure and practical consensus for blockchain based VANET. Inf Sci. 2021; 545: 170–187.
20. Xuan S, Chen Z, Chung I, Tan H, Man D, Du X, Guizani M. ECBCM: a prestige-based edge computing blockchain security consensus model. Trans Emerg Telecommun Technol. 2021; 32(6): e4015.
21. Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access. 2021; 9: 13938–13959.
22. Cachin C, Vukolić M. Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873. 2017.
23. Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. ICT express. 2020; 6(2): 93–97.
24. Kaur M, Khan MZ, Gupta S, Noorwali A, Chakraborty C, Pani SK. Mbcp: Performance analysis of large scale mainstream blockchain consensus protocols. IEEE Access. 2021; 9: 80931–80944.
25. Yu B, Liu J, Nepal S, Yu J, Rimba P. Proof-of-QoS: QoS based blockchain consensus protocol. Comput Secur. 2019; 87: 101580.

