Resilient Consensus Sustained Collaboratively

Junchao Chen, Suyash Gupta[†], Alberto Sonnino[‡], Lefteris Kokoris-Kogias[§], Mohammad Sadoghi
Exploratory Systems Lab, University of California, Davis
[†]University of California, Berkeley [‡] MystenLabs [§] IST Austria

The key goal of any blockchain system is to offer its clients a transparent and accountable ledger [6]. This ledger is maintained by multiple untrusting parties (servers) that add each client transaction to the ledger in an ordered manner by participating in a consensus protocol that can handle Byzantine attacks. Initial blockchain systems such as Bitcoin [10] and Ethereum [12] employed the *Proof-of-Work* (PoW) protocol [10, 12], which follows a *computation-oriented* consensus model. PoW protocol requires all its participants to compete toward solving a complex puzzle. Whichever participant solves the puzzle first, gets to add a new entry (*block*) to the ledger. However, PoW protocol is infamous for massive energy wastage [6].

This motivated the blockchain community to adopt two other categories of protocols: (1) Proof-of-Stake (PoS) protocols and (2) traditional Byzantine fault-tolerant (BFT) consensus protocols. PoS protocols advocate for a *stake-oriented* model where the node with the highest stake (or wealth) gets to add a new block to the ledger [3, 9]. Traditional BFT protocols advocate for an authenticated *communication oriented* architecture, where each node gets an equal chance to add an entry to the ledger; agreement on the next block is reached through successive rounds of vote exchange [2, 8]. However, all of these types of protocols suffer from *long-range attacks* [1, 4]. These long-range attacks pose unprecedented dangers; a malicious party can re-write the *full history* of the ledger.

PoS and BFT protocols suffer from long-range attacks as, in these protocols, adding a new block to the ledger is *computationally inexpensive*. Each block added to the ledger includes the digital signatures of a quorum of participants, which proves that this quorum agreed to add this block to the blockchain. To perform a long-range attack on such blockchains, an adversary needs to simply *compromise the private keys* of the honest participants. Unsurprisingly, stealing private keys is a common attack, and some of these attacks have led to losses of up to $200 million. An adversary can use these keys to create an alternate ledger; such a long-range attack can incur catastrophic losses for the impacted parties [1, 4].

Prior attempts to eliminate long-range attacks require (1) appending PoW consensus to impacted blockchain [11], and (2) increasing the number of keys an adversary needs to compromise [1]. Unfortunately, these solutions lead to substantial energy wastage or delay the imminent long-range attack. In this paper, we present an energy efficient and secure solution to resolving long-range attacks. Our novel *Power-of-Collaboration* (PoC) protocol can be easily appended to existing PoS and BFT blockchains to guard their ledgers against long-range attacks.

To guarantee a tamper-proof ledger that prevents long-range attacks, like PoW, PoC terms its participants as miners and requires them to solve compute-intensive puzzles. However, unlike PoW, PoC avoids being an energy guzzler by ensuring that no miner's work goes to waste. It does so by requiring all the miners to *collaborate* to solve the compute-intensive puzzle. This collaboration deters malicious miners from rewriting the ledger as they need more computational power than the combined power of all the honest miners. The worst malicious miners can do is avoid collaborating with honest miners. This behavior would momentarily waste the resources of honest miners but would not go unnoticed. PoC quickly identifies such malicious miners and heavily penalizes them for such behavior. Interestingly, this infrequent waste of resources comes with massive opportunities. As PoC miners collaborate instead of compete: (1) PoC is able to sustain high throughput of the original blockchain, which is a major win for PoC as PoW-based blockchains have been shown to have extremely low throughputs. (2) PoC guarantees a single blockchain, which is uncommon for PoW as the competition between its miners constantly forks the blockchain. These forks can trigger 51% attacks and require PoW-based blockchains to continuously monitor and modify the difficulty of the mining.

To show that PoC is effective in practice, we append it to ResilientDB, which runs Pbft consensus protocol among its replicas [6–8]. We select ResilientDB's Pbft implementation as it adds approximately 9000 blocks per second on a system of 4 replicas. At this high throughput, we show that our PoC is able to commit 1000 blocks per second with 64 miners. Notice that this 1000 blocks per second is a much higher throughput than a majority of state-of-the-art blockchains. We prove this by comparing against popular blockchain systems DiemBFT [5], and Ethereum [12].

REFERENCES

[1] Sarah Azouvi, George Danezis, and Valeria Nikolaenko. 2020. Winkle: Foiling Long-Range Attacks in Proof-of-Stake Systems. In *AFT*. 189–201.
[2] Miguel Castro and Barbara Liskov. 2002. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Trans. Comput. Syst.* 20, 4 (2002), 398–461.
[3] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. 2018. Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In *Advances in Cryptology – EUROCRYPT 2018*. Cham, 66–98.
[4] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Constantinos Patsakis. 2019. A survey on long-range attacks for proof of stake protocols. *IEEE Access* 7 (2019), 28712–28725.
[5] Diem Association. 2022. Diem BFT. https://www.diem.com/en-us/
[6] Suyash Gupta, Jelle Hellings, and Mohammad Sadoghi. 2021. *Fault-Tolerant Distributed Transactions on Blockchain.* Morgan & Claypool Publishers.
[7] Suyash Gupta, Jelle Hellings, and Mohammad Sadoghi. 2021. RCC: Resilient Concurrent Consensus for High-Throughput Secure Transaction Processing. In *37th IEEE International Conference on Data Engineering, ICDE 2021, Chania, Greece, April 19-22, 2021*. IEEE, 1392–1403.
[8] Suyash Gupta, Sajjad Rahnama, Jelle Hellings, and Mohammad Sadoghi. 2020. ResilientDB: Global Scale Resilient Blockchain Fabric. *Proc. VLDB Endow.* 13, 6 (2020), 868–883. https://doi.org/10.14778/3380750.3380757
[9] Sunny King and Scott Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. https://www.peercoin.net/whitepapers/peercoin-paper.pdf
[10] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[11] Ertem Nusret Tas, David Tse, Fisher Yu, and Sreeram Kannan. 2022. Babylon: Reusing Bitcoin Mining to Enhance Proof-of-Stake Security. *arXiv preprint arXiv:2201.07946* (2022).
[12] Gavin Wood. 2015. Ethereum: A secure decentralised generalised transaction ledger. http://gavwood.com/paper.pdf