QuickSync: A Quickly Synchronizing PoS-Based Blockchain Protocol

Shoeb Siddiqui†, Varul Srivastava†, Raj Maheshwari and Sujit Gujar†
†*Machine Learning Laboratory*
International Institute of Information Technology
Hyderabad, India
{shoeb.siddiqui,varul.srivastava}@research.iiit.ac.in; raj.maheshwari@students.iiit.ac.in; sujit.gujar@iiit.ac.in

***Abstract*—Proof-of-Stake(PoS) based blockchain protocols have gained popularity due to their higher throughput and low carbon footprint when compared with Proof-of-Work blockchain protocols. The two major parts of blockchain protocols are the selection of the next block proposer and the selection of the longest chain. In PoS the block publishers are selected based on their relative stake. However, PoS-based blockchain protocols may face vulnerability against Fully Adaptive Corruptions.**

This paper proposes a novel PoS-based blockchain protocol, QuickSync, to achieve security against Fully Adaptive Corruptions while improving performance. Towards this, we propose a metric for each block: block power. We compute the chain power of a chain as the sum of block powers of all the blocks comprising the chain. The chain selection rule selects the chain with the highest chain power as the valid chain. Since the block proposer is not selected upfront, this scheme is resilient to fully adaptive corruptions, which we also show formally. We also ensure that our block power mechanism is resistant to Sybil attacks. We prove the security of QuickSync by showing that it satisfies the common prefix, chain growth, and chain quality properties. Our analysis demonstrates that QuickSync performs better than Bitcoin by order of magnitude on both transactions per second and time to finality.

I. Introduction

A *blockchain* is an append-only, secure, transparent, distributed ledger. It stores the data in *blocks* connected through immutable cryptographic links, with each block extending exactly one previous block. Introduced in Bitcoin [8], blockchain is one of this century's most significant technological innovations. The underlying technical problem that Bitcoin solves through blockchain is *byzantine fault tolerant distributed consensus* in a decentralized system.

In any blockchain system, delays in communication and adversarial attacks may cause *forks* in the chain, creating ambiguity as to extend which block. The consensus protocol prevents these forks by selecting a node for publishing blocks using a *block publisher selection mechanism* (BPSM). However, forks may still occur. To resolve these forks, we require a *chain selection rule* (CSR) to choose one among them. The BPSM and CSR functionally characterize a blockchain protocol. Bitcoin blockchain protocol uses a *Proof-of-Work* (PoW) based BPSM and *longest chain* as the CSR. Typically, we measure a blockchain's performance with the two metrics: i) *transactions per second* (tps), and ii) *time for finality* (t_f), i.e., the time required to confirm a transaction.

PoS-based blockchain protocols, such as Algorand [5], and Casper [3], stochastically choose the *selected block publisher* (SBP) with probability proportional to its *relative stake*. The *Ouroboros* protocols [1], [2], [4], [6], [7] are popular PoS-based protocols, amongst others.

For a blockchain protocol to be completely secure, it must be immune to *fully adaptive corruption*s (FACs), i.e., a *dynamic adversary*. Ouroboros v1 is not immune to FACs.

In this work, we propose a novel blockchain protocol, *QuickSync* that is secure against FACs, and achieves slightly better tps, and improves on the t_f by a factor of 3, as compared to Ouroboros v1. Essentially, it quickly synchronizes (resolves) the forks that arise. To build *QuickSync*, we employ the framework of the Ouroboros protocol. *QuickSync* differs from v1 and Praos in both the BPSM and the CSR. The key idea is to propose a metric called *block power* assigned to each block. Using this, we compute the *chain power* of every competing chain as the sum of all block powers in that chain. We then establish the *best chain* with the highest chain power from a given set of chains. All forks are thus trivially resolved, except for the ones generated by the adversary. We have designed our block power to be resistant to Fully Adaptive Corruptions as well as Sybil attacks. As multiple nodes publish blocks simultaneously, it may seem that there will be several forks in *QuickSync*, as is the case in the other PoS protocols such as Praos. The key novelty here is that we resolve these forks immediately using block power.

Our Contributions. In summary, the PoS-based blockchain protocol, *QuickSync* fixes the security weakness of Ouroboros v1 and performs better in terms of tps and t_f by about an order of magnitude as compared to Bitcoin.

- We have developed a novel CSR mechanism through a Sybil-resistant function that we call block power. Our CSR mechanism is capable of an instant resolution of forks.
- We propose a simple and elegant PoS protocol that is secure against Fully Adaptive Corruptions yet highly efficient compared to other PoS-based protocols.

Note that due to space constraints, we only describe main protocol and important results. All the other details are available in our full version [9].

979-8-3503-1019-1/23/$31.00 ©2023 IEEE

Fig. 1: *QuickSync* Protocol

***QuickSync Protocol Pseudo-code*;**

Followed by node i in slot l:
INPUT: $\{sk_i^l, r_i^{ep}, seed^{ep}, S_{view(i,l)}^{Chains}, s, \{tx_0, tx_1, \ldots\}\}$
Step 1: *Chain selection*

1: From $S_{view(i,l)}^{Chains}$, select the subset $S_{view(i,l)}^{validChains} : \forall C \in S_{view(i,l)}^{validChains} | len(C) = l - 1$.
2: $\forall C \in S_{view(i,l)}^{validChains}$, calculate, $P(C)$.
3: Select the chain, $C_{csr} : C_{csr} = \text{argmax}_{C \in S_{view(i,l)}^{validChains}} P(C)$

Step 2: *Block publishing*

a) *Block building*

1: Build $Bd_i^l = \{tx_0, tx_1, \ldots\}$, and obtain $MTR(Bd_i^l)$.
2: $\{\sigma_{uro}^{i,l,seed^{ep}}, \sigma_{proof}^{i,l,seed^{ep}}\} \leftarrow VRF(sk_i^l, l, seed^{ep})$
3: Obtain $\{hash(B_{C_{csr}}^{l-1}), null(B_{C_{csr}}^{l-1})\}$
4: Build $Bh_i^l = \{pk_i, r_i^{ep}, l, \{hash(B_{C_{csr}}^{l-1}), null(B_{C_{csr}}^{l-1})\}, \{\sigma_{uro}^{sk_i^l,l,seed^{ep}}, \sigma_{proof}^{sk_i^l,l,seed^{ep}}\}, MTR(Bd_i^l)\}$

b) *Block broadcasting*

1: Set $C_{broadcast} = \{C_{csr}, B_i^l\}$
2: **while** Current Slot $== l$ **do**
3: Listen and receive C_{rec} from other nodes
4: **if** $P(C_{rec}) > P(C_{broadcast})$ **then**
5: Set $C_{broadcast} = C_{rec}$
6: **end if**
7: Broadcast $C_{broadcast}$
8: **end while**

Step 3: *Block confirmation*

1: **for** $j > 0; j++; j \leq len(C_{csr}) - k$ **do**
2: Confirm block, B_C^j.
3: **end for**

II. *QuickSync* Protocol

A. QuickSync *Security and Performance*

***QuickSync* Security Analysis.** Security of *QuickSync* follows from the following results (the proof can be found in [9]). We optimize *QuickSync* for improved performance and present a comparison of t_f and tps, between *Bitcoin*, Ouroboros v1, and *QuickSync*, in Tables I and II .

Theorem 1. *The probability that any of; common prefix with parameter k, chain growth with parameter $\zeta = 1$, and chain quality with parameter $\upsilon = 1/k$ are violated in the lifetime of the protocol, thereby violating liveness and persistence is $\varepsilon_{lp} \leq 2\varepsilon_{cp}$.*

Proposition 1. QuickSync *is resilient to* Fully Adaptive Corruptions *(FACs).*

TABLE I: Comparison of tps

	tps
Bitcoin	$\frac{tpb}{avg.timeperblock(sec)} = \frac{2000}{600} = 3.3$
Ouroboros v1	$\frac{tpb \times r^{active}}{t_{sl}} \implies tps < 50 \ \forall \ r^{active} < 1$
QuickSync	$\frac{tpb}{t_{sl}} = 50 \ \forall \ r^{active} > 0$

TABLE II: Comparison of Time to Finality (in minutes)

BTC: Bitcoin, v1: Ouroboros v1, QS: *QuickSync*

r_a \ $1-\eta$	0.99			0.999		
	BTC	v1	QS	BTC	v1	QS
0.10	40	6	2	50	10	4
0.15	40	10	4	80	16	6
0.20	70	14	5	110	24	8
0.40	580	183	55	890	296	90
0.45	2200	831	226	3400	1327	361
0.47	5970	2506	632	8330	3969	1041
0.48	-	5991	1434	-	9438	2335

III. Future work and Conclusion

PoS-based protocols are attracting attention in the literature but may potentially be vulnerable to FACs, as in v1. In this paper, we proposed a novel PoS-based blockchain protocol, namely, *QuickSync*. To design it, we introduced a block power metric resistant to Sybil attacks. We showed that *QuickSync* satisfies chain prefix, chain growth, and chain quality properties with appropriate parameters (Theorem 1). We also showed that *QuickSync* is resistant to FACs (Proposition 1). Our analysis showed that *QuickSync* performs better than the Ouroboros protocols for t_f (time to finality; by a factor of 3) and tps (transaction per second). We leave it for future work to explore the application of our BPSM and CSR to build blockchain protocols outside the Ouroboros framework.

References

[1] Badertscher, C., Gaži, P., Kiayias, A., Russell, A., Zikas, V.: Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 913–930. ACM (2018)

[2] Badertscher, C., Gazi, P., Kiayias, A., Russell, A., Zikas, V.: Ouroboros chronos: Permissionless clock synchronization via proof-of-stake. IACR Cryptol. ePrint Arch. p. 838 (2019), https://eprint.iacr.org/2019/838

[3] Buterin, V., Griffith, V.: Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437 (2017)

[4] David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 66–98. Springer (2018)

[5] Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N.: Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles. pp. 51–68. ACM (2017)

[6] Kerber, T., Kohlweiss, M., Kiayias, A., Zikas, V.: Ouroboros crypsinous: Privacy-preserving proof-of-stake. In: Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake. p. 0. IEEE (2018)

[7] Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference. pp. 357–388. Springer (2017)

[8] Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system. Working Paper (2008)

[9] Siddiqui, S., Srivastava, V., Maheshwari, R., Gujar, S.: Quicksync: A quickly synchronizing pos-based blockchain protocol (2023)