Addressing Blockchain Mutability

Jonathan Mann
jonathan.mann@nyu.edu
www.grantkey.com

May 2021

Abstract

This paper addresses the blockchain mutability problem whereby newly minted blocks are subject to reversal if they are outpaced by a competing chain meaning transactors must wait for several additional blocks to be written for the risk of transaction overturn to become negligible. This situation results in unacceptably long delays for certain types of transactions. This paper proposes a protocol where the network selects a designated validator to cryptographically sign all blocks so that a block clears as soon it is signed and the designated validator is kept honest by the fact that any act in bad faith would be almost immediately detected and a new designated validator would be selected. An implementation of a blockchain using the protocol described in this paper can be found at www.grantkey.com.

1 Introduction

Although it would be infeasible to purposely alter a blockchain backed by a sufficiently large network, the popular blockchain implementations of the present-day, which rely on consensus protocols, are not immutable [1]. By design, consensus protocols typically attempt to converge on the longest available valid blockchain, but transactions written to the blockchain can be overturned if the chain they are written to is outpaced by a competing chain. Transactions never truly settle, but, instead, have a diminishing likelihood of being overturned. As a consequence, transactors must wait for several additional blocks to be written until they believe the risk of transaction overturn to be negligible. This protocol presents unacceptably long delays for certain types of transactions [2]. This paper proposes an alternative protocol which probabilistically solves the immutability problem. The design can be described as a variation on the proof-of-stake concept which substitutes the somewhat complicated validator selection process with a simple chain of succession and where the stake is the ability to continue collecting transaction processing fees. Under the proposed protocol, the network authorizes a designated validator to serve as a system of record, cryptographically signing each block to ensure that the blockchain can never

be altered without detection. The effect is that transactions clear as soon as they are written, and, if the designated validator ever operates in bad faith, any agent producing a valid signature from the designated validator not in the blockchain will be able to prove malfeasance to the entire network and a new designated validator would be selected.

2 Constraints

Implementation of a blockchain that achieves probabilistic immutability requires that the blockchain must remain cryptographically sound throughout its lifespan. This means that a sudden advance in which cryptographic signatures become forgeable would make the protocol described in this paper unreliable. Similarly, if inter-agent communication could be successfully restricted, there would be no way to communicate malfeasance on the part of the designated validator allowing for block removal and subsequent rewrites [1]. Finally, if the validators are not appropriately incentivized to act in good faith and the benefit of defection becomes greater than the benefit of compliance, the entire system could unravel. The discussion in the incentives section addresses this component.

3 Transactions

When an agent, as identified by a public key, initiates a transaction, it must be cryptographically signed by the same agent, and, unless it is that agent's first transaction, have a timestamp greater than that of the agent's previous transaction to prevent replay attacks. The timestamp must also have occurred in the past relative to when it is evaluated since any transaction with a valid timestamp will have been minted before being submitted for evaluation. The transaction is broadcast to the network and the designated validator verifies that the agent has the appropriate digital assets to facilitate the transaction and that the agent's signature is valid. If the validation fails, the transaction is rejected and is not written to the blockchain. If the validation succeeds, the transaction is placed into a block which is signed by combining the signature of the previous block, the current block number, and the contents of the current block. As soon as the designated validator writes the block, the transaction clears. Additionally, since clearing a transaction does not depend on network-wide validation, scalability is as simple as adding processing power to the designated validator. This represents an enormous improvement over alternatives such as Ethereum which, at present, can process about 15 transactions per second [3] and Bitcoin which remains around 7 transactions per second [4].

4 Trustless Validation

Since every agent has access to the entire history of the blockchain and the validation method is publicly available any validation discrepancies will be immediately apparent. Similarly, if the designated validator ever tries to manipulate the blockchain, any agent producing a signed block not in the blockchain will be able to prove the malfeasance of the designated validator to the entire network. If the designated validator ignores valid transactions or processes them too slowly, a new designated validator can be selected by the network. Since all transactions are publicly broadcast to the network, for a portion of the network fees, secondary validators will periodically sign validation transactions confirming that the blockchain is valid and is not missing transactions. In the event that the designated validator operates in bad faith, one of these secondary validators can be selected by the network to serve as the new designated validator. Because these safeguards are in place to detect cheating, as long as the incentives are correctly aligned, the blockchain has a probabilistic guarantee of remaining immutable.

5 Chain of Succession

Although the specifics of how the network comes to agreement around choosing a new designated validator are unimportant for the purposes of this paper, one possible solution is to simply select the earliest available secondary validator appearing in the blockchain. As long as clear succession rules are agreed upon, transitioning to a new designated validator could happen seamlessly.

6 Incentives

In order for the blockchain to achieve probabilistic immutability, the incentives must be aligned such that the wrong people do the right thing. In other words, the benefits of compliance and prosocial behavior must outweigh the benefits of defection. Rather than relying on the costly practice of mining in which every node in the network competes to add new blocks and the mining computation of all non-winning nodes is wasted, closer to the proof-of-stake model, the designated validator should be rewarded with transaction fees. Because any malfeasance on the part of the designated validator would be immediately detectable by the network leading to its replacement, the designated validator would face strong incentives to act in good faith to continue collecting transaction fees. Similarly the secondary validators could be incentivized by receiving a portion of the transaction fees and also have the opportunity to be in the chain of succession in the event that the designated validator falters or acts in bad faith.

7 Conclusion

Although not for every use-case, the designated validator protocol's signature-based blockchain simplifies the staking selection process while reducing computation, storage, and clearing time costs. The reduced transaction costs pave the way for new transaction types that were not previously viable.

References

[1] D. C. de Leon, A. Q. Stalick, A. A. Jillepalli, M. A. Haney, and F. T. Sheldon, "Blockchain: properties and misconceptions," *Asia Pacific Journal of Innovation and Entrepreneurship*, 2017.

[2] M. C. Munger, *Tomorrow 3.0: Transaction Costs and the Sharing Economy*, ser. Cambridge Studies in Economics, Choice, and Society. Cambridge University Press, 2018.

[3] M. Schäffer, M. Di Angelo, and G. Salzer, "Performance and scalability of private ethereum blockchains," in *International Conference on Business Process Management*. Springer, 2019, pp. 103–118.

[4] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[5] G. J. Larios-Hernández, "Blockchain entrepreneurship opportunity in the practices of the unbanked," *Business Horizons*, vol. 60, no. 6, pp. 865–874, 2017.

[6] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[7] D. Easley, M. O'Hara, and S. Basu, "From mining to markets: The evolution of bitcoin transaction fees," *Journal of Financial Economics*, vol. 134, no. 1, pp. 91–109, 2019.