Wethio
Blockchain in Africa

Wethio Blockchain

Technical Document

Table of Content

1 ABSTRACT

This document provides a brief overview of Wethio blockchain, its architectural design, functioning, consensus protocol, and validation mechanisms. Wethio is a Proof-of-Stake Voting (PoSV)-based public blockchain which is built on top of the EVM (Ethereum Virtual Machine) protocol. Wethio blockchain is designed to back the Zynecoin cryptocurrency network in Africa and overcome complex industry challenges. It aims to incentivize cooperation amongst crypto miners and enable users to actively participate in blockchain mining for shared profits. Wethio blockchain speeds up the transaction processing cycle and deliver other benefits such as reduced transaction costs and double validation for enhanced security. It incorporates a Proof-of-Stake Voting (PoSV) consensus to provide a fair voting mechanism that ensures faster decision making. We also provide a lucrative reward mechanism for the participating nodes, ensuring fair benefits to the masternodes with a uniform probability distribution function.

2 INTRODUCTION

The blockchain network is rapidly expanding with new innovators joining in, enhancing its capabilities to serve cross-industry business applications. Blockchain is one of the most sought-after technologies which is highly in demand because of its transformative features and benefits. It is a distributed digital ledger technology that provides a secure database to store transactional data in a decentralized manner. Blockchain forms a peer-to-peer network that stores data in a series of blocks that are cryptographically linked. The data stored in blockchain is shared with all the nodes in the network to maintain an optimal level of transparency and avoid fraudulent transactions. Nevertheless, access to a blockchain can be divided on departmental basis by forming a

permissioned network. Blockchain creates an immutable and tamper-proof record of stored data that cannot be altered or deleted by any node. Besides being the backbone of the cryptocurrency network, blockchain can be used in any industry to safeguard data sources and enable fair data usage.

Wethio is an attempt to consolidate the blockchain infrastructure and create a unique ecosystem for miners, crypto enthusiasts and mainstream users. It is a collaborative effort to encourage more users to participate and benefit from mining and Wethio's unique reward mechanism. This document sheds light on Wethio's blockchain architecture and how it aims to counter the complex industry challenges with the following characteristics:

- **Improved operational efficiency:** Many popular blockchains (like Bitcoin and Ethereum) possess several performance issues and lack scalability. Wethio is designed to automatically adjust to the increasing number of users and handle average daily transactions more efficiently.

- **Faster transaction validation and processing:** The blockchains associated with Bitcoin and Ethereum take longer than usual to validate and process transactions. For Bitcoin, the average block time is significantly larger than the network latency. Wethio aims to overcome these challenges by processing high-speed transactions with double validation scheme for enhanced security.

3 WETHIO BLOCKCHAIN ARCHITECTURE

Wethio blockchain is run and maintained by a set of masternodes that operate consistently in adherence to the consensus protocol. The masternodes in Wethio blockchain are responsible for holding its

native crypto token i.e Zynecoin. To become a masternode, a coin-holder must have the minimum amount of Zynecoin tokens required (find details in the next section below). In addition, he/she must be one of the most voted candidates in the Wethio network.

Below is a neat architecture diagram of Wethio blockchain which clearly depicts the masternode network and its functioning.

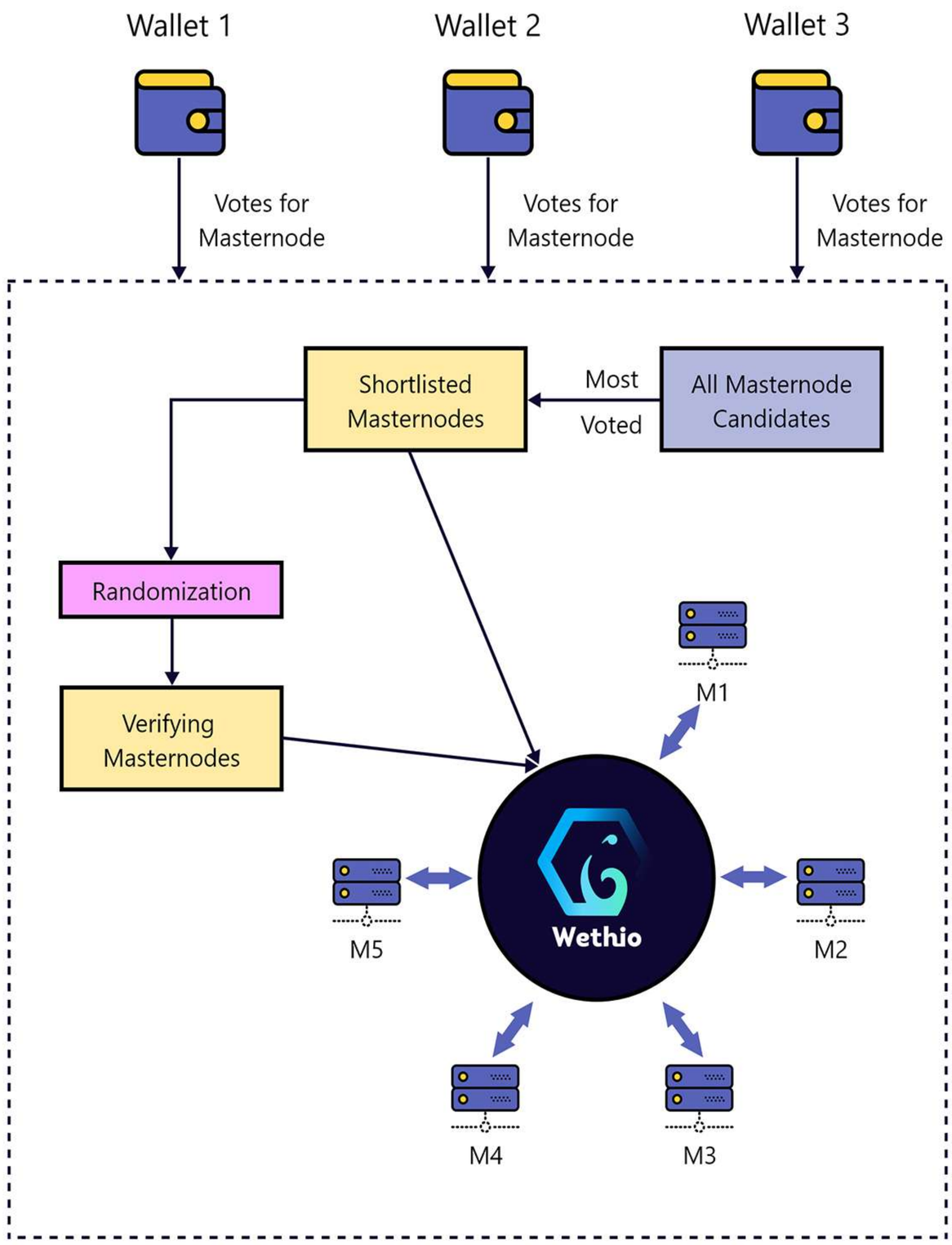

Fig. 1.1 Wethio Architecture

a) **Wethio Voting and Masternode Requirements**
   A maximum of ninety-nine masternodes can be elected in Wethio's masternode committee. The minimum amount of

Zynecoin tokens required to become a masternode is 50,000. At the time of voting, this amount is locked in a smart contract. If in any case, a masternode is removed or it intentionally quits the masternode committee, the deposit amount will be locked for a period of 30 days.

b) Mining and Reward Structure

At Wethio, we introduce a unique reward mechanism for the participating nodes. For implementing reward processing, a checkpoint block called Epoch is created for each iteration. It follows a circular sequential order to create a block where the participating masternodes scan the blocks created in the epoch. The signature count is updated accordingly by the masternode. The more signatures a masternode validates, the more rewards it earns.

Below is the custom logic for mining and reward distribution:

- **50 per cent** of the rewards' amount is reserved for the miners.
- **25 per cent** goes to the state treasury fund.
- **25 per cent** goes to the organization (Wethio).

Note: *Coin holders who unvote before the epoch will not be eligible for rewards.*

4 WETHIO BLOCKCHAIN CONSENSUS PROTOCOL

The consensus protocol of Wethio blockchain follows the concept of double validation as opposed to single validation which significantly improves the existing consensus mechanisms.

Wethio masternodes play a significant role in running and stabilizing system performance. Double validation mechanism enables full nodes to swiftly run on the available hardware configuration. This, in turn,

provides high-speed network connectivity to achieve the required block time (target to two seconds).

Below is a detailed discussion about double validation and how it enhances the network stability.

a) **Double Validation Scheme**

In the existing PoS-based blockchain networks, a masternode is responsible for creating each block. For each epoch, a single node gets permission for block creation in adherence to a pre-defined circular sequence of masternodes. On the contrary, Wethio incorporates a double validation mechanism that requires signatures from two masternodes for each block creation. Out of these two masternodes, one is responsible for block creation while the other one verifies it and adds to the blockchain. The block verifying node is randomly selected from the most voted masternodes. For increased convenience, block creation and verification functions are performed interchangeably for the proposed masternode 1 (creator) and randomly selected masternode 2 (verifier).

The double validation mechanism is critical for enhancing the stability of blockchain while maintaining the system security and efficiency. It also eliminates the probability of producing “garbage” blocks. The randomization of block verifiers in double validation is also effective at reducing risks involved with masternodes trying to create malicious blocks. Above all, the double validation technique enables Wethio blockchain to significantly reduce the block time as it requires only two signatures per block.

b) **Double Validation vs Single Validation**

Below is a detailed explanation that describes how double

validation mechanism is different from single validation.

Single Validation

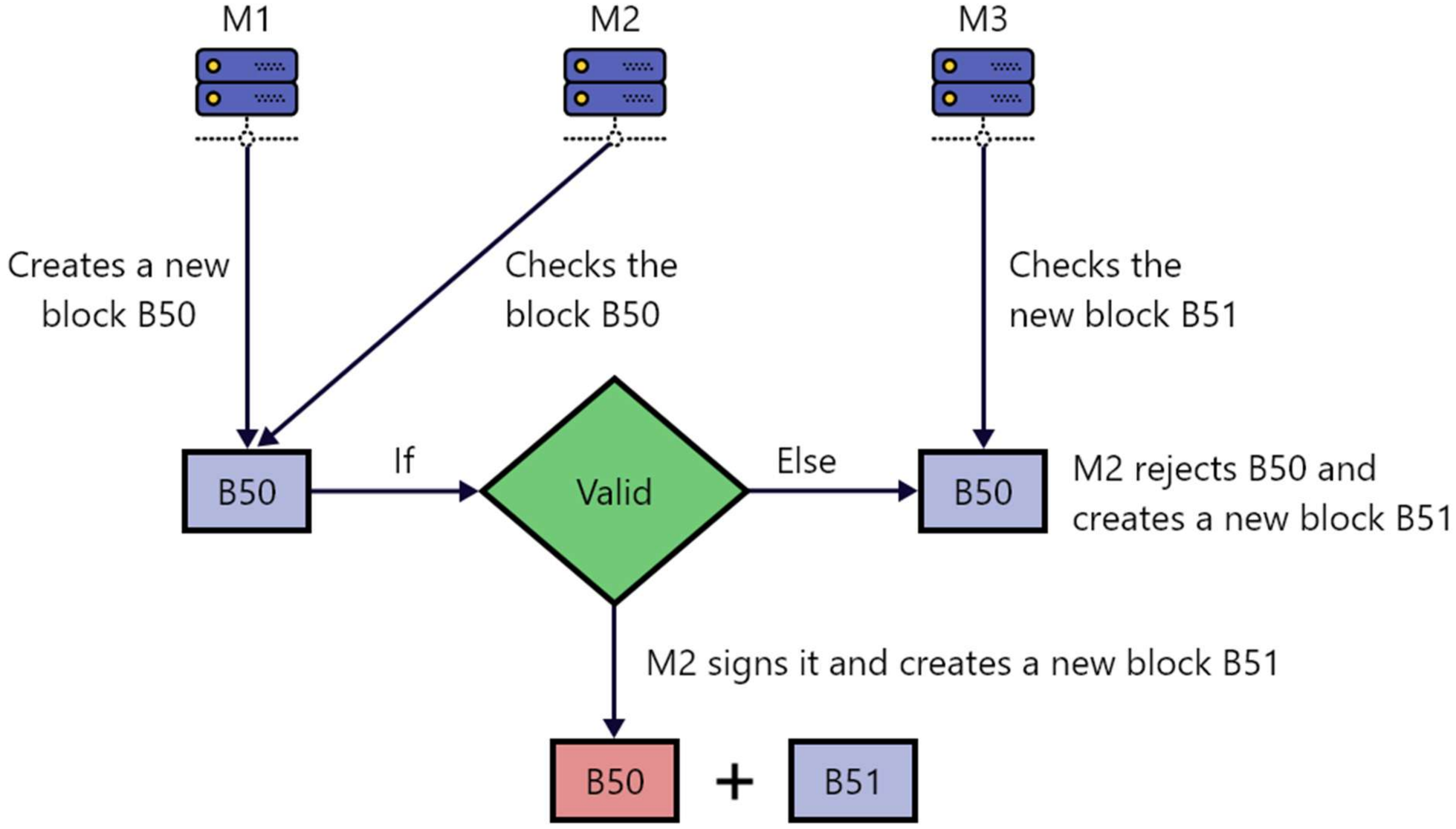

Fig. 1.2: Single Validation Case 1

In single validation, each masternode sequentially creates a block which in turn, is validated by a different masternode. For example, let's say the block B50 is created by a masternode M1 (refer to fig. 1.2). This block needs to be validated by the next masternode M2 in the same sequence. If in any case, block B50 is found invalid (i.e M1 attempts a malicious activity), M2 can reject this block and create a new block which shall be validated by the next masternode i.e M3.

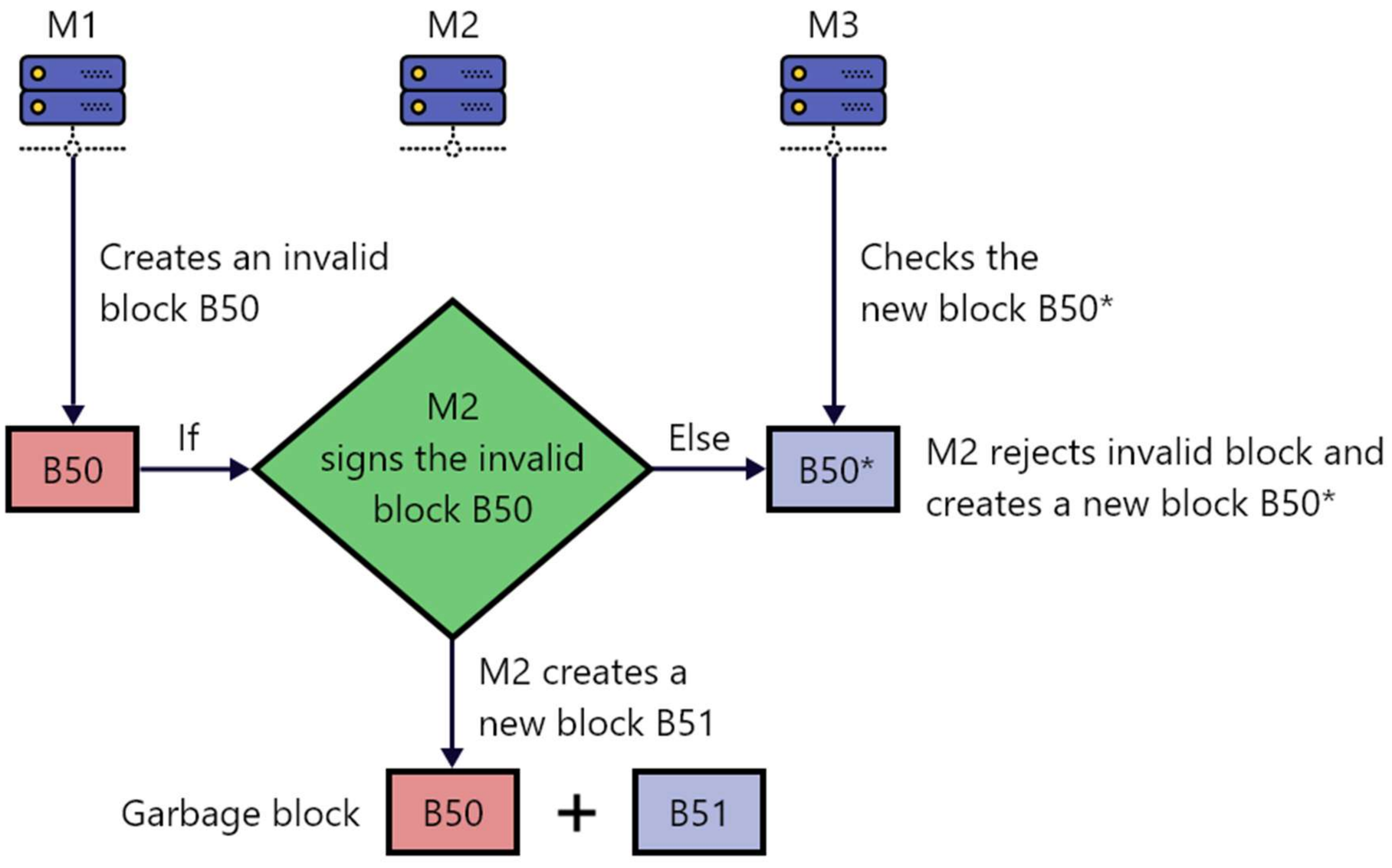

Fig. 1.3: Single Validation Case 2

However, if M2 ignores the invalid block created by M1 (refer to fig. 1.3), signs it and creates a new valid block B51, then the next masternode M3 will validate it and continue with the process of creating the next block. So in this case, it leaves blockchain with a “garbage block, B50” and it requires a “rebase” to restore the validity of blockchain.

Double Validation

The double validation mechanism significantly reduces the possibility of creating garbage blocks with the blockchain. As we saw in the previous example, if by any chance, an invalid block is ignored by a masternode, it unnecessarily creates a garbage block.

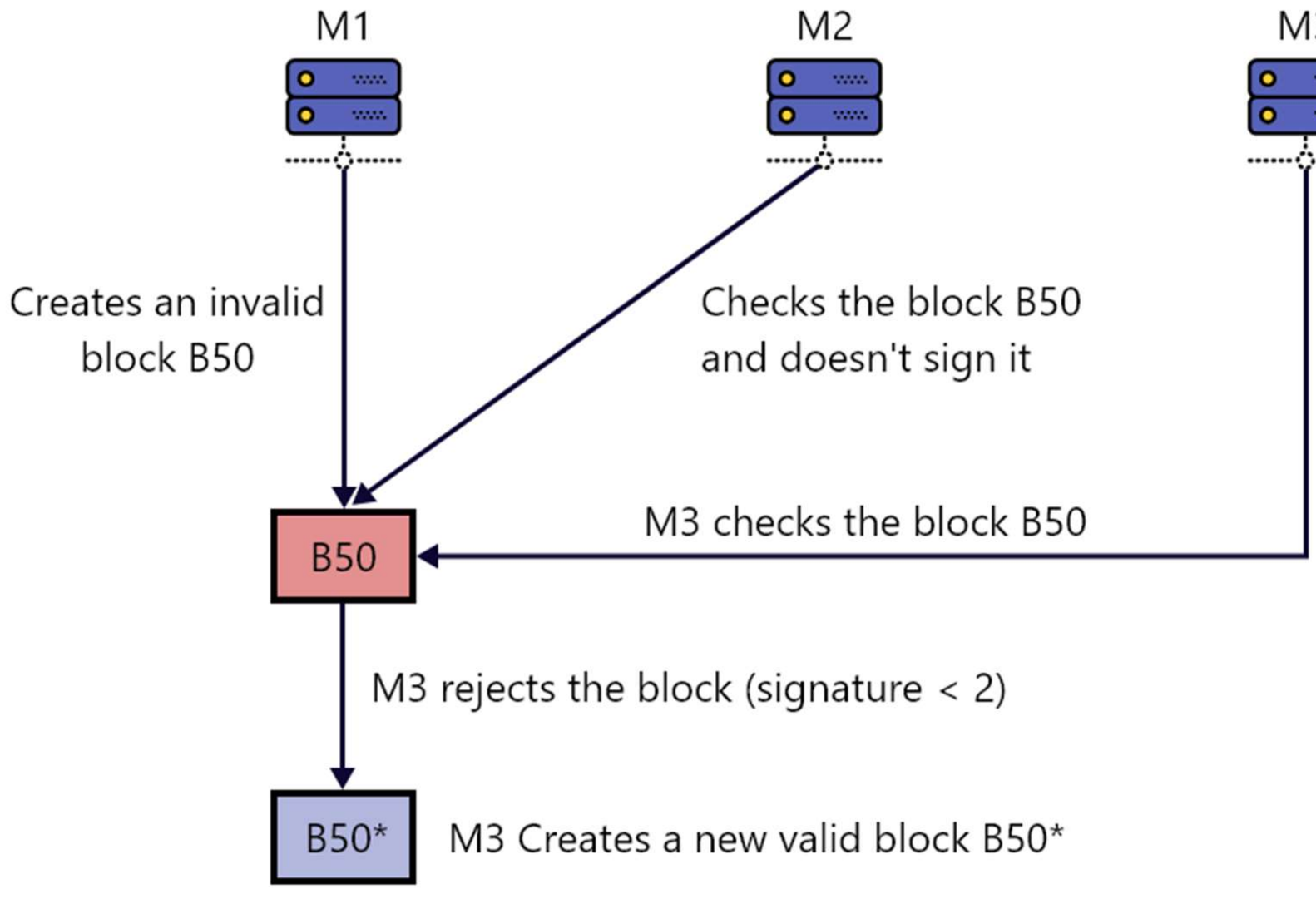

Fig. 1.4: Double Validation Case 1

In double validation, the newly created block must be signed by two masternodes for validation. For instance, let's say that masternode M1 is the creator and masternode M2 is the verifier (randomly selected). If a block B50 is created by the masternode M1, then it must be signed by both M1 and M2 for further validation. If in any case, the block B50 created by M1 is invalid, then M2 will detect it and will not provide the requisite signature. In this situation, the next masternode M3 will detect that the block B50 has incomplete signature (minimum two signatures are required for each block). As a result, M3 will reject the block B50 and will create a new block which shall be signed by M3 and M4 for further validation.

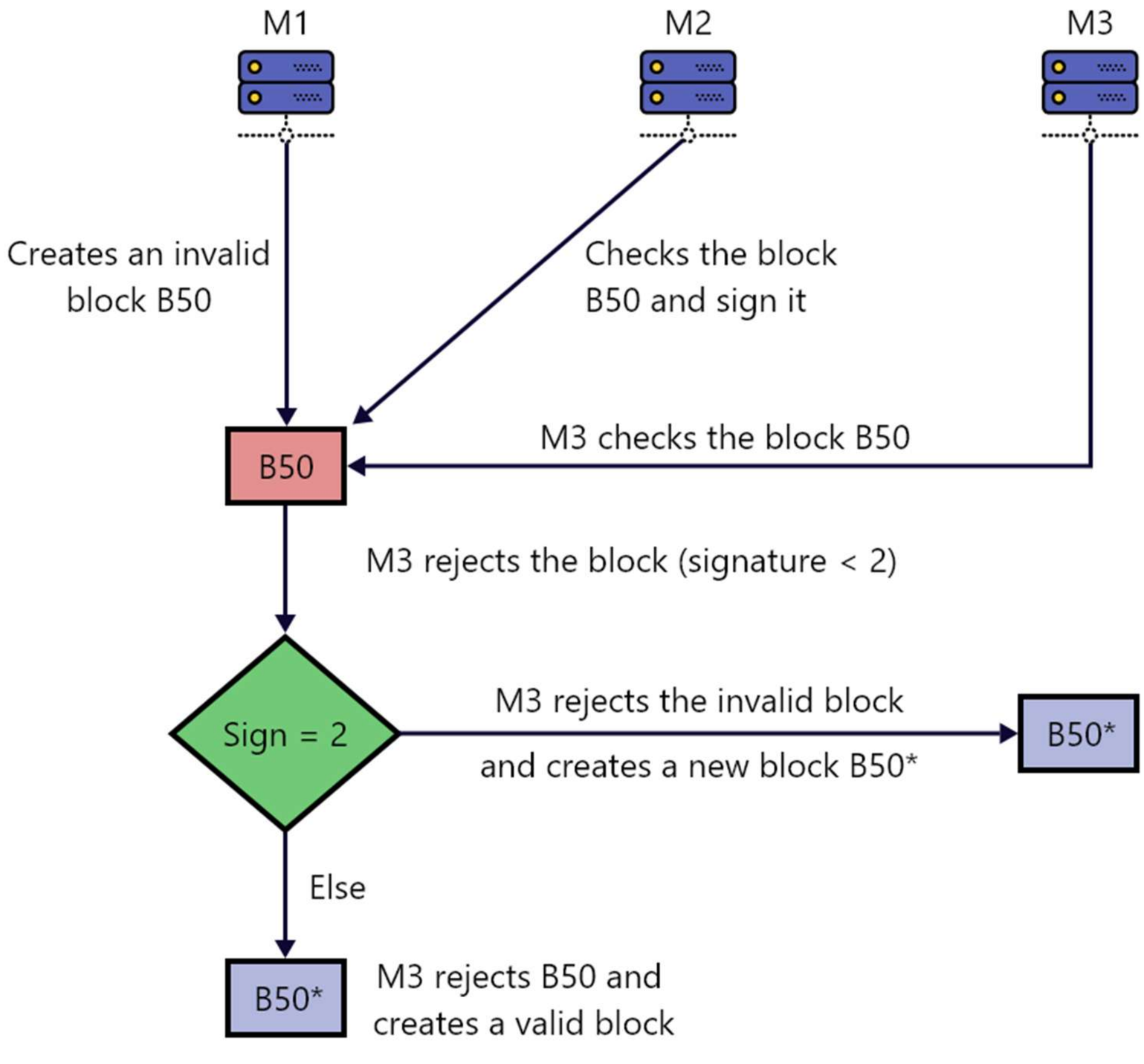

Fig. 1.5: Double Validation Case 2

Now let's assume that masternode M2 intentionally or unintentionally signs the invalid block B50, the masternode M3 will still detect it and will reject this block.

In this way, the double validation scheme provides an additional layer of security to the blockchain.

Using this validation technique, Wethio blockchain aims to strengthen its network security and significantly reduce the occurrence of malicious activities.

5 Zynecoin Wallet

Zynecoin wallet is the default wallet application for Wethio blockchain. The Zynecoin users and token holders can use this wallet to store their ZYN tokens and make transactions on Wethio blockchain. In addition, the Zynecoin wallet users can participate in Wethio consensus, vote for masternodes, track rewards, and other transactions.

Zynecoin wallet provides a simple and intuitive mobile interface for users to store, send, and receive ZYN tokens over the secure peer-to-peer connections. It also plays a critical role in the selection of Wethio masternodes as all nodes can actively participate in the voting process. The users can also track their earned rewards in real-time and maximize their profits from staking.

a) Getting Started With Zynecoin Wallet

Zynecoin wallet will soon be available on Google Play and Apple App Store. Once it's live, you may download it on the supported mobile platforms i.e Android and iOS. After downloading, you can set up a new wallet account, or restore your existing account with easy access to your ZYN tokens.

b) Metamask

Metamask is required to connect your Zynecoin wallet to the Wethio mainnet. To establish this connection, you need to install a Chrome extension on your browser (Google Chrome). After installing the extension, create an account by agreeing to the **terms of use** for metamask. Then follow the instructions specified in the extension to successfully connect your wallet to Wethio mainnet.

6 Wethio Security Analysis

Wethio blockchain is designed to speed up transaction validation and processing with an additional layer of security i.e double validation. Through Wethio, we aim to overcome several security challenges persisting in most PoS-based blockchains. To address these security vulnerabilities, we have introduced a number of security features as explained below.

Security Issues Targeted by Wethio

Cyber Attacks

Cyber attacks like DDoS, spam, and phishing are a common occurrence in most blockchain systems. Wethio blockchain incorporates an effective way to deal with spammers and prevent the network from DDoS attacks. In case of a DDoS attack, the Wethio network remains functional despite multiple node failures. The network performance in Wethio depends on the number of nodes under DDoS attack. If this number is less than 1/4th of the total number of masternodes, the network remains perfectly functional.

Spamming is possible in Wethio network as a masternode can broadcast a spammy transaction to dupe the other nodes by offering low transaction fee. However, the masternode committee in Wethio only selects the high fee transactions for the proposed block. It significantly reduces the chances of a spammer causing harm to the network.

Censorship Problems

Censorship issues is a major security concern in Ethereum and many other blockchain platforms. Since blockchain is a public and distributed

ledger, any user can store data on this P2P digital ledger without permission. However, there has to be an appropriate mechanism to govern the activities of a blockchain and eliminate censorship issues.

In Wethio, a censorship attack can happen if 3/4th of the masternodes are maliciously validating incorrect blocks. However, Wethio requires each masternode to have at least 50,000 ZYN tokens which is locked for a definite period of time. Therefore, the probability of 3/4th of the nodes becoming hostile is considerably less

Long-range attacks

Long-range attacks are quite common in PoS-based blockchain systems. These attacks cause the blockchain to start from the genesis block and override the main chain. Wethio blockchain significantly reduces long-range attacks using double validation mechanism.

Every new block in Wethio must be validated by two masternodes. Therefore, the network remains perfectly functional as long as the number of malicious masternodes remain less than ¼ the total number of masternodes.

7 Conclusion and Future Prospects

This technical document highlights the key value propositions of Wethio blockchain and how it aims to address the complex industry challenges with PoSV protocol. It also sheds light on Wethio consensus protocol and how it facilitates fair voting within the network for masternode selection. In the later sections, we discussed the reward mechanism and double validation scheme for faster transactions and secure transaction processing. After reading this documentation, you

must be able to download and install Zynecoin Wallet and then connect it to Wethio mainnent. As we move further, we aim to introduce more advanced features in Wethio blockchain to strengthen its security, privacy, and operational efficiency. We are also working on improving the scalability of our blockchain to accommodate an increasing number of users and enable them to make high-speed transactions over the secure P2P channels.

**Please note that this is the first version of the document and is subject to changes as new features are implemented in Wethio blockchain.*

Reference

1) Tomochain - Staking on Masternodes Wars. Altcoinbuzz. March 3, 2019.

2) How Masternodes Work. Dash Technical Document. 2018.

3) What is Delegated Proof-of-Stake (DPoS). Lisk Academy. October 2019.

4) Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism. IEEE. August 2019

5) Tomochain - Staking on Masternodes Wars. Altcoinbuzz. March 3, 2019.

6) R. Pass, L. Seeman, and A. Shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. EUROCRYPTO. 2017.

7) Delegated Proof-of-Stake (DPOS). BitShare White Paper 2014.

8) Rewriting History: A Brief Introduction to Long Range Attacks. Evangelos Deirmentzoglou. May 31, 2018.

9) Understanding the Basics of a Proof-of-Stake Security Model. Interchain Foundation. Nov 2, 2017.