Core DAO: The Decentralization of Bitcoin with the Expressiveness and Composability of Ethereum

The Core DAO Team
coredao.org

Version 1.0.5

Abstract

This paper proposes a new, independent blockchain to operate at the core of Web 3. Powered by a new consensus mechanism, Satoshi Plus, Core is a Turing-complete blockchain leveraging the Bitcoin mining hashrate and the Ethereum Virtual Machine (EVM). Satoshi Plus applies a protocol-driven validator election mechanism to combine the optimal features of Proof of Work (PoW) and Delegated Proof of Stake (DPoS) in order to ensure the maximization of security, scalability, and decentralization.

1 Introduction

The Blockchain Trilemma is a well-studied problem by both academics and market participants. It states that all cryptocurrencies, including Bitcoin, Ethereum, etc. must make trade-offs between optimal security, scalability, and decentralization, often prioritizing two elements at the expense of the third, as demonstrated in Figure 1,

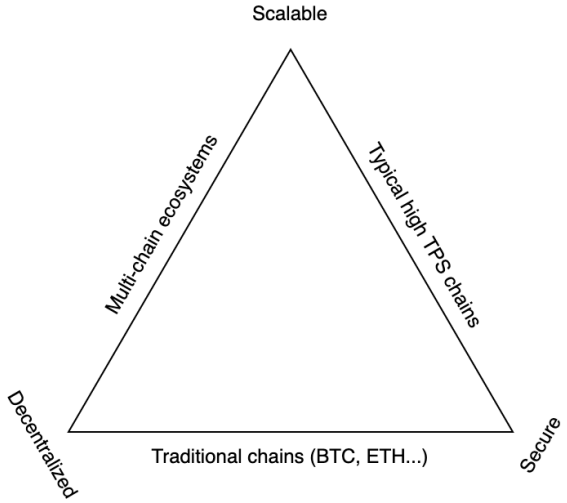

Figure 1: Blockchain Trilemma
https://bit.ly/391b2m2

Our solution to the trilemma above is Satoshi Plus consensus, which operates at the core of the Core Network. Satoshi Plus consensus combines Proof of Work (PoW) and Delegated Proof of Stake (DPoS) to leverage the strengths of each while simultaneously ameliorating their respective shortcomings. Specifically, Bitcoin computing power guarantees decentralization, the DPoS and leadership election mechanisms ensure scalability, and the entire network holistically maintains its security. Core is the first chain to implement our new consensus mechanism. Although it will not be the last, we believe that with the strength of our community, CORE will achieve the necessary network effects required to create a successful currency and serve as the much needed springboard for broader Web 3 adoption.

The rest of the paper is organized as follows. First, we compare the tradeoffs made by other L1 and L2 networks. Next, we dig deeper into Satoshi Plus consensus and its various components. We then discuss the security properties and future directions for the Core network. We then discuss the base layer currency of the chain - CORE. Finally, we discuss the governance of the Core

network via the Core DAO.

2 Background

2.1 Related Works

2.1.1 Bitcoin

In 2009, Satoshi Nakamoto carved scarcity out of the stone of abundance. Despite its enablement of infinite replicability, the internet could now have its own native currency on the blockchain: Bitcoin - the first truly digital solution to the problem of money [Nak]. Bitcoin introduced PoW mining to the world, allowing anyone with compute power to participate in securing the network. Leveraging Nakamoto consensus, Bitcoin has become the most decentralized blockchain, but with only 7 TPS, it lacks the scalability [Aut] necessary to transition beyond "Store of Value" use cases. BTC's role as "digital gold" is unquestioned, but as the hype around the Lightning Network illustrates, many in the Bitcoin community want more.

2.1.2 Ethereum

The most popular dapp platform and the first Turing-complete blockchain [Buta]. The abstractions offered by the Ethereum Virtual Machine (EVM) and the popular Solidity programming language allowed hundreds of thousands, if not millions, of developers to build decentralized applications for the first time [She], which has given rise to DeFi, Play2Earn, NFTs, etc. Ethereum offered a higher TPS than Bitcoin at the expense of some decentralization, but even with its 15 TPS, major scalability bottlenecks remain [Fri].

2.1.3 Ethereum 2

The catchall term for the community driven upgrades to Ethereum meant to resolve the scalability, security, efficiency, etc. challenges. Two of the major changes are the move from PoW to PoS and the introduction of sharding. Sharding purportedly will offer up to 100k TPS [RK], but the migration to PoS draws concerns regarding decentralization [You]. Already, we are witnessing significant concentration among major CeFi custodians such as Binance, Kraken, etc and staking pools like Lido.

2.1.4 Solana

A high TPS chain, 50k TPS, that leverages both Proof of History (PoH) and sharding [Yak]. Solana has very short block times, 400ms [Tead], which allows applications built on top of the network to feel like Web 2 in terms of performance. In order to achieve this level of performance, the requirements to run a validator far exceed most other networks [Teae], thereby pricing out many players. Another tradeoff exists between performance and network availability, which has been visible more recently with a few notable chain restarts [McS] [Mil]. Solana also has one of the most active developer communities, but the transition to Rust from Solidity has proved challenging for many.

2.1.5 Polygon

An L2 scaling solution built on top of Ethereum meant to solve many of the scalability challenges on the main chain by leveraging PoS and side chains [Teac]. Polygon has attracted a sizable number of developers given its EVM compatibility, which allows dapp developers to port over their code with minimal to no changes [Teab]. Polygon faces criticisms regarding the lack of decentralization and stability of its validator set, which has thus far remained unchanged since testnet, although they are actively working on improving these dynamics with Polygon DAO [Rze].

2.1.6 Binance Smart Chain

A hard fork of the Go Ethereum (Geth) codebase. One of the major differentiators between BSC and Ethereum is BSC's Proof of Staked Authority (PoSA), a consensus mechanism that combines Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) [Teaa]. By leveraging this new consensus mechanism, BSC achieved faster transaction times, higher TPS, and lower fees [CZ]. Since its inception, BSC has faced criticism regarding insufficient decentralization given that its validator set is more or less fixed given the 3rd parties' relationship with Binance and the high stake requirements (minimum $2.3m USD or 10,000 BNB vs Ethereum 2 $32k USD or 32 ETH as of July 2022) combined with the fact that only 2 of the 21 are involved in consensus activities at a given time [Tra]. The claim that Binance itself runs any of the nodes can be disproven via onchain data [BsC].

2.1.7 Comparisons

	Scalable	Decentralized	Secure
Bitcoin	✗	✓	✓
Ethereum	✗	✓	✓
Ethereum 2	✓	✗	✓
Solana	✓	✗	✓
Polygon	✓	✗	✓
Binance Smart Chain	✓	✗	✓
Core (Satoshi Plus Consensus)	✓	✓	✓

Figure 2: Comparison of related works.

2.1.8 Evolution of Go Ethereum

Core is an evolution of the Geth codebase. We leveraged the improvements made by the BSC team to add greater throughput and cheaper transactions by way of hard fork. Nevertheless, we differ from BSC in many ways. One

preeminent difference is that Core is based on Satoshi Plus Consensus, which relies on Proof of Work (PoW) alongside Delegated Proof of Stake (DPoS). With these modifications, we're able to remain decentralized without the performance tradeoffs seen in traditional PoW consensus systems. Additionally, with our hybrid score based off of both delegated Bitcoin hash power and delegated stake, we've created a fluid market for validators and rewards that anyone can participate in.

3 Satoshi Plus Consensus

3.1 Illustration

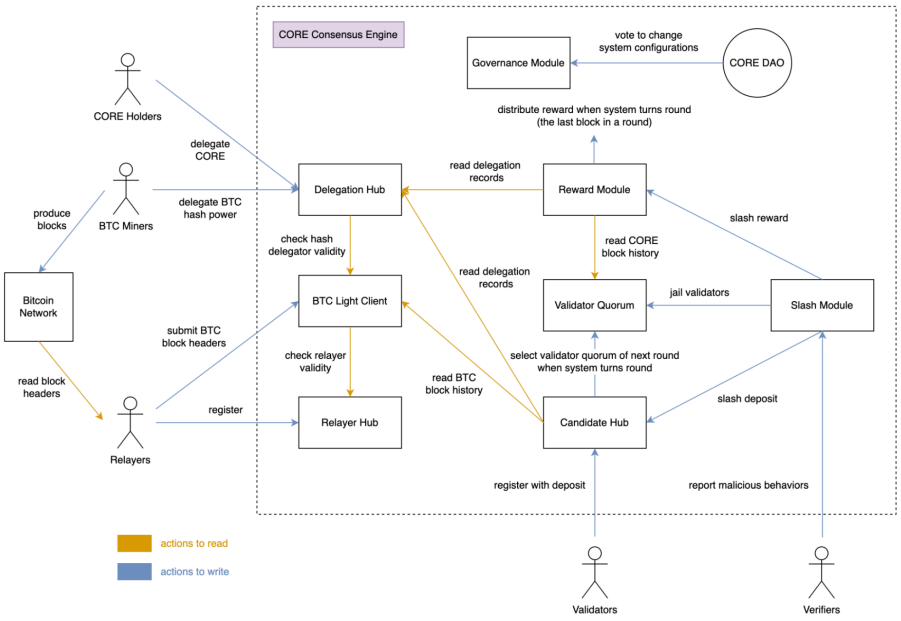

Figure 3: Illustration of major roles and components.

3.2 Major components, roles, and workflows

Validators: Responsible for producing blocks and validating transactions on the Core network. Becoming a validator requires registration with the network and locking up a refundable CORE deposit to be included into the validator set per the rules of the validator election. Anyone can deposit and become a validator on Core.

Relayers: Responsible for relaying BTC block headers to the Core network. In order to relay, a potential relayer must register with the network and lockup a refundable CORE deposit. Anyone can deposit and become a relayer on Core.

BTC Miners: The miners responsible for securing the Bitcoin network via PoW. In order to have their hash power factor into Satoshi Plus consensus, miners must delegate their hash power to a validator that either they or a third party run. Delegation is a non-destructive act, meaning that by delegating on Core they're re-purposing their existing work vs choosing between securing Bitcoin and securing Core.

CORE Holders: Holders of the CORE currency, the base currency of the CORE chain. All holders of CORE are able to participate in staking by delegating their holdings to a validator.

Verifiers: Responsible for reporting malicious behaviors on the network. Anyone can act as a verifier in the Core network. Successful verification flags may result in slashing (rewards or stake) or jailing misbehaving validators.

Validator Election: The mechanism in which the top 21 validators are selected for inclusion in the validator set. Validators are elected in relation to their hybrid score each round.To ensure a more stable TPS, the "live" validators are updated every 200 blocks during the round so that other validators do not need to wait for "jailed" validators for the entirety of the round.

Hybrid Score: The output of the protocol function used in validator election calculations. The inputs to the function are the BTC hash power and CORE delegated to the validator.

Round: Cycle time for Core to update validator quorum and distribute rewards, which is currently set to 1 day. Each day, 21 validators with the highest hybrid scores are elected to the validator set, thereby becoming responsible for producing blocks on the Core network for the entirety of the round. At the last block of each round, the accumulated rewards for the round will be calculated and distributed and the validator quorum for the next round will also be determined.

Slot: Each round is divided into slots and all validators in the quorum take turns producing blocks repeatedly in a round robin manner until the end of the round. Currently, the slot length is set to 3 seconds. In each slot, an honest validator either produces a block or fails to do so.

Epoch: The cycle length for the system to check each validator's status to exclude jailed validators from the quorum to prevent them from participating in the consensus to keep TPS more or less constant in a given round. Currently, epoch is set to 200 slots, which is 600 seconds or 10 minutes.

3.3 Proof of Work

Proof of Work is a practical mechanism for implementing a decentralized network. PoW is non-discriminatory and allows anyone who owns compute power to participate in mining. Leveraging the existing BTC mining network, Core relayers transmit each Bitcoin block as a transaction to the Core chain. This relaying mechanism is how Satoshi Plus validates delegated hash power in a

trustless fashion. With this PoW element, Satoshi Plus is able to leverage the security of the Bitcoin network to secure Core.

3.3.1 Relayers

Relayers in Core are responsible for relaying BTC block headers onto the network via the on-chain light client. Relayers must both register and pass verification in order to receive rewards.

3.3.2 BTC Miners

Using their public and private keys, BTC miners can delegate their hash power to a Core validator or delegate to themselves if they choose to run a validator by verifying and syncing their identity (addresses) on both the BTC and Core blockchains. When relayers submit transactions, they sync the blocks mined by the BTC miner with the Core Network. Every round, the Core network calculates the BTC hash power associated with each validator by counting the number of blocks produced by each miner in the BTC network during the same day of the prior week. The architecture of the mapping-chain communication is illustrated in the diagram below.

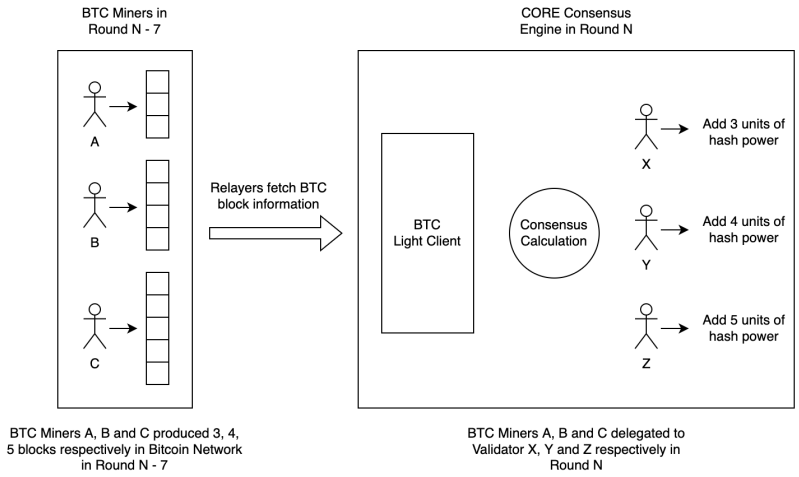

Figure 4: BTC Miner Hash Power Relaying.

3.4 Delegated Proof of Stake

Proof of Stake is a scalable, energy-saving alternative to PoW, but it restricts small stake users. In an attempt to level the playing field, some blockchains have introduced various types of Delegated Proof of Stake (DPoS) mechanisms, allowing the token holders to vote and elect the validator set by delegating their holdings to validators, typically incentivized by rewards. Using DPoS,

even small-stake CORE holders can delegate their CORE to validator candidates, which empowers the community and incentivizes the democratization of delegated CORE.

3.5 Validator Election

3.5.1 Overview

Core's validator election adheres to the following mechanics:

1. Hybrid scores are calculated for all validators in the network. The function to calculate the scores is defined as:

$$S = rHp/tHp * m + rSp/tSp * (1 - m) \quad (1)$$

where: rHp = hash power delegated to validator, which is measured via the count of BTC blocks produced
tHp = total hash power on Core
rSp = stake delegated to validator, which is measured via the amount of CORE token delegated
tSp = total stake on Core
m = is a dynamic weighting that adjusts over time to ensure a smooth transition during ramp up

2. Select the 21 validators with the highest hybrid scores to be included in the validator set.

3. The election takes place at the end of each round to pick up validators for the next round via the mechanism above.

3.5.2 Block Production

Satoshi Plus validator election is designed to select validators deriving from both the PoW and DPoS methods outlined above. After election, the mechanism sorts all validators and produces blocks in a round-robin manner. By round robin, we mean that every validator has a chance to produce a block in a strict ordering, from 1-21 ranked by hybrid score before it restarts again from the top. Additionally, by limiting the number of validators, Satoshi Plus offers a higher transaction rate and increased scalability. Furthermore, this mechanism provides additional resistance to various attacks with improved efficiency and tolerance of a certain number of Byzantine players (malicious or hacked).

3.5.3 Validator Self Regulation

Core contains slashing and jailing mechanisms to disincentivize malicious behavior by validators in each round. While producing blocks, the existing Core validators check if any current validator has been jailed periodically. If so, they will update the validator set after an epoch period. For example, if Core produces a block every three seconds and the epoch period is 200 blocks, then the current validator set will check and update the next epoch's validator set in 600 seconds (10 minutes). The design of the jailing is to exclude illbehaving validators from consensus activities in order to enhance network security and keep TPS stable.

3.6 Rewards

3.6.1 Illustration

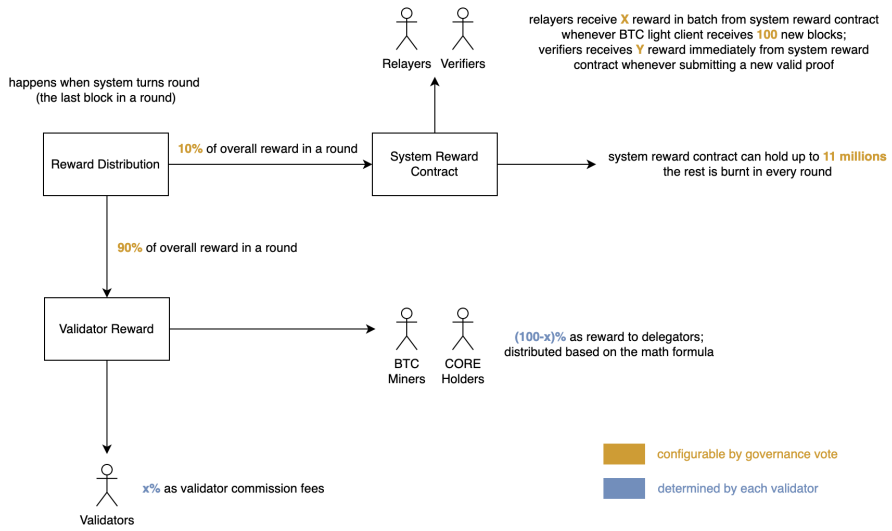

Figure 5: Illustration of Rewards Workflows.

At the last block of a round, rewards are calculated and distributed. Currently, 90% of the rewards go to the validators and 10% of the rewards go to the System Reward Contract. Of the 90% paid to validators, some percentage (x%) is taken as a commission by the validator before paying out their delegates. The System Reward Contract accumulates rewards to pay out both relayers and verifiers with a current maximum cap of 11 million of accumulated CORE rewards (10m relayer rewards and up to 1m verifier rewards that are self-replenishing) before burning excess rewards. Verifiers are paid immediately upon successful submission and relayers are paid every 100 BTC blocks.

3.6.2 Node Rewards and Distribution to Delegators

The two categories of rewards for validators are (1) base rewards (newly minted CORE) and (2) fees collected from transactions in each block. Validators are required to share rewards with the delegators who staked their CORE with them in addition to those delegating hash power. Given each validator has an equal probability to produce blocks, in the long run all stable validators should get a similar portion of the reward.

Validators can decide how much to give back to the delegators who delegated their CORE or their hash power with them. These validators are incentivized to greatly reward their delegators in order to attract more hash power and stake. After taking their fees, the protocol uses a function to determine the split between staked rewards and hash power rewards for a validator defined as:

$$rH = rHp/tHp * m/S * R \tag{2}$$

$$rS = rSp/tSp * (1-m)/S * R \tag{3}$$

where: rH = validator rewards attributed to hash power
rS = validator rewards attributed to staking
R = overall rewards attributed to all delegators

$$rHu = rH/rHp \tag{4}$$

$$rSu = rS/rSp \tag{5}$$

where: rHu = validator hash power rewards per unit
rSu = validator staking rewards per unit

Note that these functions are designed to create an active market for rewards and encourage competition amongst the validator set for both delegated hash power and delegated stake. By the same mechanism, delegators will try to optimize their own rewards by choosing validators with lower amounts of delegated hash power and stake.

3.6.3 Applied Example of Node Rewards and Distribution

Let's assume there are 2 validators and both are elected:

- A: 2 units of hash power, 1 unit of stake
- B: 1 unit of hash power, 4 units of stake

Let's also assume there are 10 total units of BTC hash power on the Core network, so validator 1 has 20% of the hash power and validator 2 has 10% of the hash power. Similarly, we assume there are 20 total units of stake on the CORE network, so validator 1 has 5% of stake and validator 2 has 20% of stake. We also set m to $\frac{2}{3}$ for this example.

For the simplicity of the calculation, we set the number of earned rewards to distribute to 1 for both validators.

Scores:

$$S_A = 2/10 * 2/3 + 1/20 * 1/3 = 9/60 \tag{6}$$

$$S_B = 1/10 * 2/3 + 2/10 * 1/3 = 8/60 \tag{7}$$

Rewards:

$$rH_A = (2/10 * 2/3)/S_A = 8/9 \tag{8}$$

$$rS_A = (1/20 * 1/3)/S_A = 1/9 \tag{9}$$

$$rH_B = (1/10 * 2/3)/S_B = 1/2 \tag{10}$$

$$rS_B = (2/10 * 1/3)/S_B = 1/2 \tag{11}$$

Reward per Unit:

$$rHu_A = rH_A/2 = 4/9 \tag{12}$$

$$rSu_A = rS_A/1 = 1/9 \tag{13}$$

$$rHu_B = rH_B/1 = 1/2 \tag{14}$$

$$rSu_B = rS_B/4 = 1/8 \tag{15}$$

3.6.4 Relayer Rewards

Relayers earn a portion of the base system rewards and transaction fees for cross-chain communications. All rewards are deposited directly into relayers' accounts as the only communication type is Bitcoin header synchronization. Relayer rewards are distributed in batches every 100 BTC blocks.

3.6.5 Verifier Rewards

CORE slash suggestions can be submitted by anyone and ensure that malicious and harmful actors are punished. The transaction submission requires evidence and fees, but accurate submissions earn rewards that exceed the costs. Rewards are paid out immediately from the System Rewards Contract, in the same transaction, when successful.

4 Security

4.1 Overview

A high-level categorization of various attack vectors can be broken down into network attacks and consensus attacks.

1. Core mitigates network attacks (DDoS, Eclipse, BGP Hijack, etc) through a combination of transaction filtering, geographic dispersion of nodes, and random node selection for P2P communications as well as an officially published seed list for public nodes.

2. Consensus attacks are more interesting and have a wider taxonomy of threat vectors. Our combination of PoW, DPoS, and our validator election mechanism provide us with many desirable properties. Pre-computation and selfish mining are not actionable by a fixed validator set in a round-robin manner because they are attempting to manipulate a pseudorandom mechanism which does not exist on Core. Censorship and transaction delays are actionable but are mitigated as long as there are honest validators in the set. In a similar vein, some attacks like 51% and Sybil attacks can't be fully mitigated, but both are economically unwise to attempt and very difficult to achieve given our ranking by the hybrid score of their hash power and stake. Long range attacks are mitigated by our checkpointing scheme and reliance on PoW, which doesn't suffer from this category of attack. With checkpointing in place, the most relevant category of attacks are various short-range attacks (long-range + checkpointing = short range).

4.2 Short-Range Attacks

Short-range attacks come in a variety of forms, but in summation, they are aimed at rewriting a small number of blocks rather than all the way back to Genesis. Some notable examples are bribery attacks, liveness denial, and race attacks. Below, we present a mathematical proof stating that as long as less than $\frac{1}{3}$ of the nodes are malicious and enough blocks are confirmed, transactions on Satoshi Plus are definitely safe.

4.2.1 Mathematical Proof

In this section, we demonstrate that Satoshi Plus is secure if less than one-third of the validators are adversarial. We begin by examining the actions of potential enemies. What is the adversary's "ideal" strategy, and what could they achieve? We assert that the one-third bound is tight by presenting an idealized attack method: Under some attack, the system is compromised if the adversary takes more than one-third of the validator seats. Anything less than one-third would be unsuccessful. Thereafter, we discuss the logic behind our proof as well as the methodology of *proof by contradiction*. Finally, we present the formal proof, which explains the claimed outcomes mathematically.

4.2.2 The Balanced Attack

In this section, we consider the ways to increase the likelihood of a safety violation from an adversarial standpoint. We present one method for carrying out a double-spending attack. In this attack, the adversaries manage to keep a second blockchain hidden and release it when attacking. The double-spending attack is successful if the revealed blockchain is longer than the current longest public blockchain. To accomplish this, the adversaries must take advantage of the protocol and manipulate the honest blocks in such a way that they assist in the attack without violating the protocol. For example, they can keep the attacking and legal blockchains as balanced as feasible, as demonstrated in Figure 6,

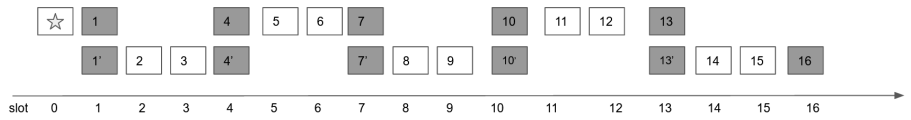

Figure 6: Successful attack with one-third adversarial validators.

3 validators are in this attack, one of which is adversarial. The attack target is the block on slot 0 (with a star sign). Block 1 is originally hidden during the attack. The block with the star and block $1'$ are visible to honest validators, and they are oriented to generate the new block, block 2, on top of block $1'$. The attacker then generates another block 4 on top of block 1, publishes it, then generates block $4'$ and hides it at slot 4. As a result, when honest validators observe two blockchains of the same height at slot 5, they are motivated to generate a new block, block 5 on top of block 4, and so on. With this strategy, the two blockchains may be kept balanced for as long as feasible with only

one adversary. A user's transaction is not secure no matter how long they wait. Even though 16 slots have elapsed in our example, the targeted block is reverted if the adversary decides to perform assault at slot 16.

4.2.3 Methodology

Let's dive into the attack strategy in part 4.2.2 to get a sense of what a successful attack looks like. Each honest validator, as we know, generates exactly one block in its slot. In this attack, two adversarial blocks are generated at an adversarial validator's slot and contributed to two blockchains. The idea is to maintain a balance between the two blockchains. As a consequence, at each height, a matching pair of blocks is required. Assume block $1'$ is the start of the attack and has the same parent as the block with the star in our scenario. The height of block 4 is equal to that of block 3, whereas block $4'$ is equal to that of block 5. Block $7'$ corresponds to block 6, while block 7 corresponds to block 8.

The key to a successful attack is for each adversary to generate two blocks in their respective slot and match them to two separate honest blocks. The "one-match-two" pattern illustrates why, for a successful attack, the adversarial to honest validator ratio must be at least $1:2$, implying that the safety guarantee is one-third of adversaries. Is the adversary capable of more? Is it possible to construct three adversarial blocks in one slot and match them to three honest blocks? The answer is no. The reason for this is that the two adversarial blocks formed at the same slot must match two honest blocks, one of which is generated before the slot and the other after the slot. To match to three honest blocks, two adversarial blocks must match two honest blocks generated both before and after the slot, which is not possible. The next section will include a formal proof.

The major technique we use is *proof by contradiction*. To prove something by contradiction, we assume that what we want to prove is not true, and then show that the consequences of this are not possible. That is, the consequences contradict either what we have just assumed, or something we already know to be true.

4.2.4 Formal Proof

We assume the total number of validators is N, among which m validators are honest and the remaining validators are adversarial. Then,

$$m > \frac{2}{3}N. \tag{16}$$

According to the protocol, we adopt a discrete model where actions take place in slots. If a validator publishes one or more blocks in a slot, all validators receive the block(s) by the end of the slot. A validator is said to be honest if it always follows the protocol. Each validator is either honest or adversarial. A block is said to be honest (resp. adversarial) if it is generated by an honest (resp. adversarial) validator. Evidently, by the end of each slot, all honest validators are fully synchronized. Honest validators only generate new blocks on top of the longest published blockchain(s) at their own slots. A blockchain is said to be honest in slot r if it is the longest blockchain as seen by some honest validators in slot r. When mentioning a blockchain, we always assume the blockchain is legal (i.e., accepted by honest validators) according to the protocol. Define an honest validator slot to be a slot where the legal generator is an honest validator.

By saying blockchain b, we mean the blockchain ending with block b. Let $T(b)$ denote the slot in which block b is generated. The height of block b, denoted as $h(b)$, is defined as the number of blocks (including the genesis block) in the same blockchain. Then we have

Lemma 1. *Honest blocks have identical heights.*

Proof. This is a simple consequence of the fact that all honest generators have seen the same blocks and every honest validator adopts the longest blockchain at the end of every slot. □

Lemma 2. *Suppose two adversarial blocks, block a and block b, satisfy $T(a) = T(b)$ and match two honest blocks c and d, then $(T(a)-T(c))(T(a)-T(d)) < 0$. That is to say, the two honest blocks cannot be generated both before or after the slot of the adversarial blocks.*

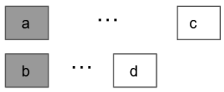

Figure 7: Illustration of Lemma 2.

Proof. Contrary to the claim, assume the blocks c and d could be generated both before or after slot $T(a)$. Without losing generality, assume they are generated after $T(a)$. By definition, by claiming block a matches to block d (block b matches to block c, respectively), we have $h(a) = h(d)$ ($h(b) = h(c)$, respectively). By the protocol, since honest block c is generated after block a on the same blockchain, we have $h(c) > h(a)$ (and $h(d) > h(b)$, respectively). Thus, we have,

$$h(a) = h(d) > h(b) = h(c) > h(a). \tag{17}$$

Contradiction arises, thus the proof. □

Note that as a consequence, one adversary can match at most two honest blocks during one slot.

An adversarial sequence is defined as a sequence of consecutive adversarial validators as ranked by the protocol. We say an adversarial block matches an honest block if they are at the same height of different blockchains.

Lemma 3. *The adversarial blocks generated by an adversarial sequence of n validators match at most $2n$ honest blocks.*

Proof. This is a natural extension of Lemma 2 □

A block is said to be *permanent* after slot r if the block remains in all honest blockchains starting from slot r. Basically, if a user transaction is permanent, the user can safely believe their transaction will not be reversed no matter what the adversaries do in the future.

Theorem 4. *If an honest block b remains in an honest blockchain in slot $T(b)+N$, then block b is permanent.*

Proof. We prove the desired result by contradiction. For simplicity let $r = T(b)$. Let n be the number of adversaries in the N validators.

Contrary to the claim, assume $s \geq r+N$ is the smallest slot when there exist some other honest blockchain d_1 which does not include block b. Then there exists another honest blockchain d_2 in slot $s-1$ containing block b. Then $h(d_2) \leq h(d_1)$. Let k be the number of adversarial sequences in the first N validator rank starting from slot r. Let $n_1, n_2, \ldots, n_k$ be the number of validators in each adversarial sequences. We have $\sum_{i=1}^{k} n_i = n$ and $k \leq n$. Let function $M(n_i)$ represent the number of honest blocks matched by adversarial sequence n_i. Then, we have $M(n_i) \leq 2n_i$ by Lemma 3. Let $\ell = \lfloor \frac{s-r}{N} \rfloor$, then ℓ is a positive integer since $s - r \geq N$. Let k' be the number of adversarial sequences starting from slot $r + \ell N$ ending in slot s. Then $n_1, n_2, \ldots, n_{k'}$ are the number of validators in the adversarial sequences during slot $[r + \ell N, s]$.

Note that since there are k' adversarial sequences, there are at least $\sum_{i=1}^{k'} M(n_i)$ honest validators during slot $[r + \ell N, s]$ to separate the sequences. Thus the total number of honest blocks during $[r, s]$ is at least $\ell m + \sum_{i=1}^{k'} M(n_i)$. Note that each honest block has identical heights according to Lemma1, thus the height increase of blockchain d_1 and blockchain b_2 are both at least

$$\ell m + \sum_{i=1}^{k'} M(n_i) \tag{18}$$

blocks are generated and included in the two blockchains during slot $[r, s]$.

On the other hand, we calculate the maximum number of blocks that the adversaries can match in the two blockchains. Each adversarial sequence with n_i validators contributes $M(n_i)$ blocks to match the honest blocks in the two chains. Thus, the total number of honest blocks being matched is

$$\ell \left(\sum_{i=1}^{k} M(n_i) \right) + \sum_{i=1}^{k'} M(n_i) \leq 2\ell \sum_{i=1}^{k} n_i + \sum_{i=1}^{k'} M(n_i) \tag{19}$$

$$\leq 2\ell n + \sum_{i=1}^{k'} M(n_i) \tag{20}$$

$$< \ell m + \sum_{i=1}^{k'} M(n_i). \tag{21}$$

Contradiction arises with equation 18. □

4.2.5 Summary of Security and Finality

Based on the mathematical proof in the previous section, we conclude that as long as a transaction is confirmed by more than N blocks, where N is the size of the elected validator set, it can never be reversed. We have also proven that to perform an attack successfully, a minimum of $\frac{1}{3}$ of the validators must be adversarial.

Note that the adversarial model used in the proof is extremely strict. The adversaries in the proof's model are assumed to be operating in conditions of perfect coordination and are placed in perfect slots in the set to compromise

honest validators in a 1:2 ratio. In this case, they also have the ability to induce honest validators to choose the required block to perform the attack when there are 2 blocks with the same block height.

In reality, the conditions mentioned above are very unlikely to occur and in some cases are impossible. Core has implemented strong punishments on various malicious behaviors to disincentivize validators to conduct such behaviors. As a result of these countermeasures, for normal transactions on Core, $\frac{1}{2}$N block confirmations should provide enough safety. For more critical transactions, we recommend $\frac{2}{3}$N+ block confirmations. For the most pessimistic case, N block confirmations will achieve 100% safety.

4.2.6 Slash-able cases

Core has managed to mitigate most attacks by various means outlined throughout this document. Our proof above provides strong guarantees that with enough block confirmations we are always safe. However, we also chose to implement slash + jail/ejection mechanisms to further disincentive malicious behaviors. Verifiers can submit evidence to have validators slashed and jailed for different cases. Two notable cases that are slash-able are double signing and unavailability.

5 Future Explorations

5.1 Scaling and Cross-Chain

Where Core is fully EVM compatible, we can leverage scaling solutions from Ethereum and other compatible chains, ex various types of rollups. We also may choose to go down a Polkadot or Cosmos style L0 relay vs hub chain model. The future of scaling is bright, and we plan to incorporate the best technologies from other chains as research matures.

5.2 Enhanced Security:

While the round-robin nature of block production provides certain security benefits, it also involves tradeoffs. For example, by having a known ordering in advance, the protocol isn't susceptible to an entire category of potential randomness exploits, but the block-producing validator is fully known which may lead to more focused attacks. In response, we are focusing on ways to improve block production. Particularly, the research around single secret leader election [HG] that chains like ETH are also exploring is of great interest.

6 CORE

6.1 Sound Supply

Following Bitcoin's sound money model, CORE's supply has a hard cap of 2.1 billion tokens. On top of the hard cap, a percentage of all block rewards and transaction fees will be burned similar to Ethereum's "Ultra Sound Money" model. The exact percentage to be burned will be determined by the DAO.

In effect, CORE will asymptotically approach the total of 2.1 billion tokens but never fully reach it, similar to Avalanche's tokenomics model.

6.2 Emissions Curve

The block rewards for CORE will be paid out over an 81 year period. This longer period increases the likelihood of the success of the chain by fully incentivizing all network participants before transitioning to compensation purely by transaction fees. This additional block reward in the form of CORE can also be thought of as a way for existing BTC miners to continue receiving subsidies after the Bitcoin block rewards are stopped (around 2040) by becoming validators on the Core network leveraging their existing hash power.

7 Governance

7.1 DAO

Until Core reaches the point of sufficient decentralization, the Core team is charged with overseeing the network through their control of the DAO. Functions include, but are not limited to altering the number of validators, regulating governance parameters, and setting the percentage of block rewards and transaction fees that are burned. The DAO's membership will continue to expand and once sufficient decentralization arrives, early CORE holders are tasked with creating and maintaining a community that believes in the Core mission and the sustainability of the network. Core is not limited to any particular vision or ideology. Diversity is our strength. We're a crypto melting-pot made possible by our simple, core goal: Secure, scalable, and decentralized digital currency for an internet based on freedom, transparency, and self-sovereignty. All are welcome.

7.2 Progressive Decentralization

Decentralization is not limited to the consensus level. Governance of the entire Core Network will progressively decentralize as time passes. At the DAO's genesis, limits on decentralization will be necessary to get the CORE chain off the ground and establish product-market fit. As the network expands, the Core DAO will increasingly lean on community participation [Wal]. Over time, the broader CORE community will gain control of all governance functions including management of the CORE Treasury.

7.2.1 Challenges

Decentralized governance is very difficult in practice due to various attack vectors [Butb]. Until the chain is mature, DAOs building on top of Core are at risk of an arbitrary Core fork overriding their governance. For the Core DAO to be successful, trust and community building are essential at the beginning of the chain's lifecycle.

7.2.2 Objectives

Core Network Maintenance objectives at the outset of this project are simple:

1. Provide a phased path towards decentralization.
2. Minimize risk to encourage DAOs to form on top of Core.

7.2.3 Decentralization Phases

Core governance via the Core DAO will progressively decentralize throughout three stages of development:

1. Off-chain governance.
   (a) Pass resolutions with a majority of DAO voters in agreement.
2. Limited on-chain governance.
   (a) Allow changing a fixed parameter set (TBD) with onchain coin voting, ex. percentage of burned fees.
   (b) Likely add time delays to discourage vote buying and similar attacks.
   (c) Adding / subtracting parameters is at the sole discretion of of the DAO voters, ex. Core Improvment Proposals (CIP).
3. Full on-chain governance.
   (a) Up to the community.

8 Conclusion

This paper has presented Core DAO, the decentralized network that we believe will serve as the nucleus of Web 3. Our consensus mechanism, Satoshi Plus, combines PoW and DPoS to resolve the oft discussed "Blockchain Trilemma". Our improvements in regards to scalability, security, efficiency, and decentralization alongside our EVM compatibility unlock the power of decentralized applications for everyone - developers, users, etc.

CORE, the base layer currency of the Core network, will be overseen by the DAO. Through its provable scarcity, contraction mechanism, governance, etc. CORE aims to become both the value accrual and usability layer for all decentralized applications.

9 Glossary

Proof of Work (PoW): A consensus mechanism using mathematical puzzles that require energy expenditure to incentivize network participants to verify transactions and add the next block to the blockchain.

Proof of Stake (PoS): An energy efficient consensus mechanism that validates transactions by selecting validators in proportion to the value of their staked holdings.

Delegated Proof of Stake (DPoS): A version of Proof of Stake consensus in which users of the network delegate tokens to stakers that validate the next block.

Ethereum Virtual Machine (EVM): Turing-complete virtual machine that enables smart contracts on Ethereum and other EVM compatible chains.

References

[Aut] Wikipedia Authors. *Bitcoin scalability problem.* URL: https://en.wikipedia.org/wiki/Bitcoin_scalability_problem. (accessed: 08.07.2022).

[BsC] BsCScan. *Top 25 Validators by Blocks.* URL: https://bscscan.com/stat/miner?range=14&blocktype=blocks. (accessed: 08.07.2022).

[Buta] Vitalik Buterin. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.* URL: https://ethereum.org/en/whitepaper/. (accessed: 08.07.2022).

[Butb] Vitalik Buterin. *Moving beyond coin voting governance.* URL: https://vitalik.ca/general/2021/08/16/voting3.html. (accessed: 08.07.2022).

[CZ] CZ. URL: https://twitter.com/cz_binance/status/1346000721313861632?lang=en. (accessed: 08.07.2022).

[Fri] Tim Fries. *Explained: Ethereum's Scalability Problems and Growing Backlash.* URL: https://tokenist.com/explained-ethereums-scalability-problems-and-growing-backlash/. (accessed: 08.07.2022).

[HG] Dan Boneh Saba Eskandarian Lucjan Hanzlik and Nicola Greco. *Single Secret Leader Election.* URL: http://www-cs-faculty.stanford.edu/~uno/abcde.html. (accessed: 08.07.2022).

[McS] Michael McSweeney. *Solana blockchain validators restart network after transaction stoppage.* URL: https://www.theblock.co/linked/117711/solana-blockchain-validators-restart-network-after-transaction-stoppage. (accessed: 08.07.2022).

[Mil] Mike Millard. *Solana restarted after seven-hour outage caused by surge of transactions.* URL: https://www.theblock.co/linked/144639/solana-restarted-after-seven-hour-outage-caused-by-surge-of-transactions. (accessed: 08.07.2022).

[Nak] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* URL: https://bitcoin.org/bitcoin.pdf. (accessed: 08.07.2022).

[RK] Stephen Graves Rene Millman and Liam J. Kelly. *What Is Ethereum 2.0? Ethereum's Consensus Layer and Merge Explained.* URL: https://decrypt.co/resources/what-is-ethereum-2-0. (accessed: 08.07.2022).

[Rze] Mateusz Rzeszowski. *State of Governance: Decentralization.* URL: https://blog.polygon.technology/state-of-governance-decentralization/. (accessed: 08.07.2022).

[She] Maria Shen. *Electric Capital Developer Report (2021)*. URL: https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d. (accessed: 08.07.2022).

[Teaa] BSC Team. *Binance Smart Chain*. URL: https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md. (accessed: 08.07.2022).

[Teab] Polygon Team. *Bring the World to Ethereum — Polygon - Polygon*. URL: https://polygon.technology/. (accessed: 08.07.2022).

[Teac] Polygon Team. *Ethereum's Internet of Blockchains*. URL: https://polygon.technology/lightpaper-polygon.pdf. (accessed: 08.07.2022).

[Tead] Solana Team. *Scalable Blockchain Infrastructure: Billions of transactions counting — Solana: Build crypto apps that scale*. URL: https://solana.com/. (accessed: 08.07.2022).

[Teae] Solana Team. *Validator Requirements*. URL: https://docs.solana.com/running-validator/validator-reqs. (accessed: 08.07.2022).

[Tra] James Trautman. *BNB Chain: The Evolving Juggernaut*. URL: https://messari.io/article/bnb-chain-the-evolving-juggernaut?utm_source=substack&utm_medium=email. (accessed: 08.07.2022).

[Wal] Jesse Walden. *Progressive Decentralization: A Playbook for Building Crypto Applications*. URL: https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management. (accessed: 08.07.2022).

[Yak] Anatoly Yakovenko. *Solana: A new architecture for a high performance blockchain v0.8.13*. URL: https://solana.com/solana-whitepaper.pdf. (accessed: 08.07.2022).

[You] Sage D. Young. *Will a Proof-of-Stake Ethereum Lead to More Centralization?* URL: https://www.coindesk.com/layer2/2022/05/18/will-a-proof-of-stake-ethereum-lead-to-more-centralization/. (accessed: 08.07.2022).