# Space Network

# Distributed Supercomputing Network

Table of Contents

## 一、Overview

With the advent of WEB3.0, centralized proprietary services are being replaced by decentralized open services; vulnerable location addresses are being replaced by resilient content addresses; and inefficient monolithic services are being replaced by peer-to-peer decentralized algorithmic markets. These systems represent the first instances of open services on the internet, forming a decentralized network of participants. Several early researchers in blockchain technology, united in Silicon Valley, initiated the SPACE Network protocol and established the Space Network Labs. In May 2018, the laboratory launched Space Network as the first implementation of the protocol.

Space Network has established a decentralized supercomputing network protocol, utilizing the [Privacy SPACE Protocol] to encourage more nodes to contribute their privacy computing power, privacy storage space, and network resources. This empowers Space Network with robust computing capabilities and efficient storage space. Users can acquire sufficient privacy computing power and storage space from Space Network by consuming a certain amount of gas. Each node in Space Network serves as a contributor to the SPACE network ecosystem, providing computational and storage contributions, participating in block packaging, witnessing and recording transactions, and receiving rewards from the SPACE network. Space Network Labs has also introduced the [SPACE Notarization Rules] to enhance privacy protection for users. Through the [SPACE Notarization Rules], zero-knowledge notarization can be applied to judgment results, ensuring privacy and decentralized absolute notarization services.

At the same time, Space Network is also an open and inclusive blockchain network. Through innovative consensus protocols, it can be compatible with the majority of computing and storage devices, as well as IoT devices. As long as the corresponding data computing power unit is satisfied, any device can join this vast network, providing computational and storage support to the entire network, achieving interconnectivity. The network implements a decentralized network with privacy through encryption algorithms, merging a massive scale of computational power and storage. Contributors are rewarded for their contributions. This network seamlessly allows users to access any unit-level privacy computing power and storage space when needed. In this aspect, it shares significant similarities with the FILCOIN network of the IPFS protocol.

Note: The SPACE Notarization Rules refer to the user's ability to customize independent contract protocols through the contract mechanism of the Space Network and publish them on the Space Network. Using the intelligent computing power of Space Network, smart contracts published on the network undergo notarization judgments. The results are notarized according to the subject matter, and the outcomes are provided to the users. Through zero-knowledge algorithms, critical information is deciphered, ensuring real-time synchronization with real-world results and guaranteeing the efficiency and accuracy of judgment outcomes.

## 二、 Protocol Laboratory

### 1.Laboratory Background

#### 1.1Laboratory Founders

Adam Back, a cryptographer from the United Kingdom, is one of the founders of the cryptocurrency "Hashcash," a precursor to Bitcoin, developed in 1997. He has emerged as a thought leader in Bitcoin development and established the blockchain technology company Blockstream in 2014. Back is among the eight individuals cited by Satoshi Nakamoto in the initial Bitcoin whitepaper. Other co-founders include Jeremiah Wagstaff (Co-founder and CEO of Space Network Labs) and Dr. David Tse (Professor of Electrical Engineering at Stanford University).

### 1.2 The Origin of the SPACE Network

Adam Back believes that processing massive data requires immense computing power, storage space, and robust network resources as support. The team led by Adam Back needed a vast, convenient, unrestricted, secure, private, decentralized, and cost-effective network ecosystem to access technological resources for research. Just like an infinite SPACE, anyone can contribute to SPACE, and individuals can obtain everything they need through the SPACE ecosystem. It is a vibrant, sustainable, and green ecosystem. Adam Back, along with his core technical research team, collaborates with geeks and scientists from around the world, establishing the SPACE Network Laboratory: Space Network Labs.

### 2.Key Events and Plans of Space Network Labs

January 2018: Establishment of Space Network Labs.
May 2018: Space Network Labs secures $5 million in venture capital from Silicon Valley investors.
March 2019: Space Network V1.0 enters the development phase.
March 2021: Completion of the development of Space Network V1.0, entering the testing phase.
April 2022: Completion of the development of Space Network V1.0 and deployment online.
May 2022: Official launch of the Space Network Space Plan.
October 2022: Space Network V2.0 Beta goes live, releasing open-source foundational code.
December 2022: Launch of DEFI projects on Space Network.
January 2023: Launch of decentralized cross-chain aggregation trading platform on Space Network.
March 2023: Launch of metaverse projects on Space Network.
June 2023: Launch of DAO ecosystem applications on Space Network.
December 2023: Initiation of BOC Notarization Platform Plan on Space Network.
January 2024: Launch of DAPP Notarization Platform (BOC Platform) on Space Network.
May 2024: Launch of APP Wallet Notarization Platform (BOC Platform) on Space Network.
August 2024: Launch of new ecosystem on BOC Platform on Space Network.

## 三、 Privacy SPACE Protocol

### 1.The Technical Principles of the SPACE Network Protocol

SPACE Network consists of different hardware devices, categorized into F nodes and T nodes. All F nodes form independent interconnected networks. Following the Space Network protocol, the system links all devices to create a decentralized supercomputing network. According to the Space Network protocol, M samples will be randomly selected following specified rules, and consensus will be reached on N out of the M samples, forming a self-aware network.

2.Consensus Mechanism in the SPACE Protocol Network

In RF-DPOS, each consensus message carries the signatures of nodes that have already reached consensus, enabling the transport and confirmation of consensus information. This allows for further optimization of the PBFT transmission protocol, making message transmission resilient to adverse transmission conditions and ensuring more stable operation.

Space Network's consensus protocol introduces innovation by adding a signature queue to the existing BFT-DPOS protocol. This allows nodes to carry consensus requests from other nodes, accelerating the efficiency of transaction and block consensus while improving consensus security. The introduction of randomness makes the system's security more reliable.

Because in Space Network, a block is generated every 10 seconds, Space nodes are required to produce and distribute proof to the network. Only when the majority of tree nodes in the network validate the proof will it be added to the blockchain. Subsequently, Space Network full nodes update contributors' space information and delete invalid records. Therefore, the computing power of Space nodes can be determined by accumulating and verifying the distribution of records from tree nodes. For Space nodes, this information can be obtained by accumulating all distribution records from the genesis block to the current block. Meanwhile, tree nodes can obtain information from trusted Space nodes.

The distribution records from Space nodes, sorted in the hash tree from the latest block header to the genesis block, ensure their authenticity and integrity through Merkle paths. This way, tree nodes can upload verified data evidence to the network. If a node maliciously forges its computing power, it needs to forge its distribution proof, which involves executing a send operation and forging false proof onto the blockchain. Since send undergoes a verification process, a successful send operation implies a genuine proof.

Space Network breaks the consensus rules of blockchain through consensus innovation. It adopts the separation of block and transaction consensus, each operating independently. SPACE-DPoS, the [Random SPACE Dynamic Migration DPoS Mechanism], is pioneered as a new consensus mechanism.

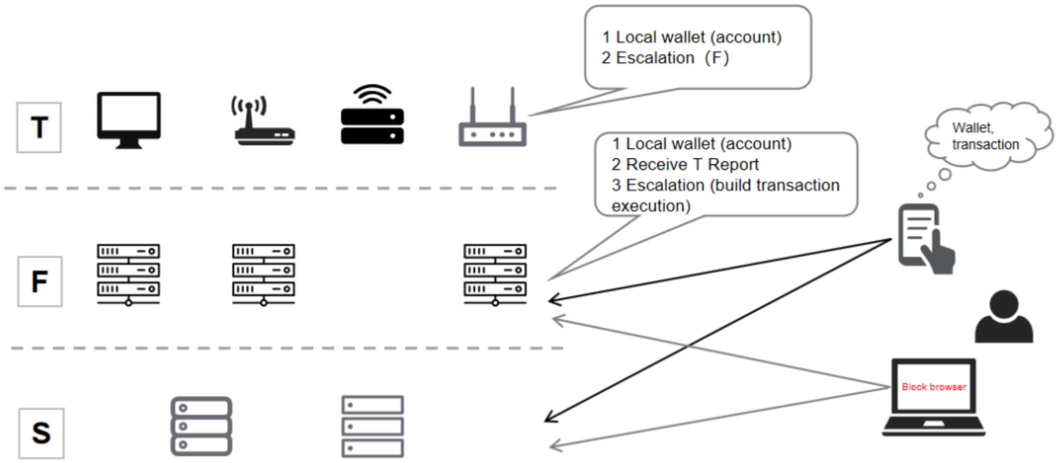
## 四、 Introduction to the Space Network

1.What is the Space Network

Space Network (Decentralized Supercomputing Network) refers to the integration of distributed computers, storage, and IoT devices with blockchain to establish a decentralized supercomputing network. Space Network enables the acquisition of trusted computing and storage resources, creating a standardized platform for data collection, computation, analysis, transactions, and notarization, providing supercomputing power and storage.

## 2.Role Description

In Space Network, the core roles constructed and maintained are the Governance Committee, Space Nodes, and Tree Nodes.




### 2.1 Governance Committee

The Governance Committee (GC) is a set of 51 nodes elected based on votes within Space nodes, representing the consensus of the entire network and maintained by these 51 GC nodes. The rotation cycle of GC nodes involves elections every 100 days. The election formula is as follows:

$$\text{AllLuckyNodeTickets} = \sum_{n=1}^{51} \text{NodeNTickets}$$

$$\text{TopNTikets} = \text{TOPNTickets} + \frac{\text{TOPNTickets}}{\text{AllGCNodeTickets}} \text{ All Node Tickets } 10\% \quad (0<N<52)$$

Election of Bookkeepers

Bookkeeper = select(order(NodeTicketsTop,RANK(a-z,0-9)),[Right(Num_Block,1)]$^3$,NodeN))

When the mainnet is not yet launched: Initial single-node consensus, blocks are generated but not rewarded. When the mainnet is already launched: For each block generation, 33 nodes are randomly selected from the 51 Governance Committee nodes for verification. Consensus is achieved, making the block/transaction irreversible.

Irreversible_(block,transaction) =IF>=Top51×67%,” YES” ,” NO”

Special case: If the number of Space nodes is less than 33, the entire network stops generating blocks.

### 2.2 Space Nodes and Tree Nodes

In Space Network, two types of nodes are established to provide architecture services for the mainnet: Space Nodes and Tree Nodes, representing the relationship between SPACE and trees in the ecological network. Space Nodes, also known as F nodes, are primarily responsible for collecting transactions in the network, transferring computing power to the mainnet, providing storage space, and receiving rewards. The existence of F nodes forms the foundation of the network. Tree Nodes, or T nodes, are used to verify transactions and record them, providing computing power units to F nodes. F nodes package transactions into blocks.

A complete Space node requires at least 3 Tree nodes to jointly maintain its normal operation, forming a legitimate FCO (SPACE Contributor Organization) that provides computing power units to the mainnet. It can be understood as a mining organization.

### 2.3 Selection of Node Lucky Value

In Space Network, when electing Space nodes to perform tasks such as data retrieval, data distribution, and block packaging, the selection is based on the lucky value of each Space node. To ensure that Space nodes of various lucky value levels have the opportunity to be selected and to leverage the effect of lucky values, the following strategy is adopted:

Lucky values are classified into levels, and the initial election is conducted based on lucky value levels. The higher the lucky value level, the higher the probability of being selected.

After the initial election, nodes with the same lucky value level undergo a uniform probability election.

The process is as follows:

Rank Space nodes based on their lucky values across the entire network and calculate probabilities.

The first block of a new round is generated by the Space node with the highest rank. The last digit of the block height determines the base number, ranging from 0 to 9. Each time an F-producing node is selected, the cube of the last digit is used as the base number. Starting from the ranking of the previous block-producing node, the ranks are cumulatively added down to determine the next node to produce a block. When the cumulative rank exceeds the total number, it loops back to the beginning. If the last digit is 0 or 1, the node itself produces the block, and subsequent nodes ranked behind it will produce blocks in turn. After producing a block, the remaining block production count of the node is reduced by 1. When the remaining count becomes 0, the node only participates in ranking and probability calculations, without producing blocks.

When calculating Space nodes for the next block, if a node is not online, the block production reward is retained, and the next ranked node (node B) produces the block. The remaining block production count of node B is reduced by 1. After block production, the three-cubed rule continues:

a) If the node is online, it continues to produce blocks until completing 16 blocks.

b) If the node is not online, the remaining block count is distributed to other nodes, similar to distributing to a pool. Blocks are produced in a cyclical manner, and each time a block is produced, the remaining block count is reduced by 1.

c) If the offline node is detected to be back online, return to (a).

This process ensures a dynamic and fair distribution of block production opportunities based on lucky values among Space nodes in the Space Network.

### 2.4 Single Node Clustering Implementation

Space Network adopts a microservices architecture, deploying clusters to implement single-node functionality. It utilizes virtualization technology with K8S+Docker for automated operations and maintenance. This allows Space nodes to have the capability of horizontal scaling and dynamic resource addition, achieving high-performance hardware capabilities.

## 3.Functional Layering

Space Network divides its functionality into different layers, including the access layer, scheduling layer, transaction layer, contract layer, transaction consensus layer, block layer, and storage layer. Each layer can run independently and be deployed in a clustered manner, ensuring high-level load balancing. This design provides Space Network with infinite scalability in software architecture.

## 4.Transaction Correlation Analysis

Space Network, in order to enable parallel execution of transactions, conducts transaction correlation analysis to determine the execution order of transactions. In the design of contracts, correlation analysis fields are added to the contract invocation interface when generating contract calls. This approach ensures that transaction analysis is universal and allows Space Network to maintain performance even as the number of contracts increases without decreasing the performance of individual contracts.

## 5.Design of Weak and Strong Correlation in Data

Space Network's transaction parallelism extends beyond transaction correlation analysis to include analysis of contract data. The data is categorized into weakly correlated and strongly correlated data. Transactions involving weakly correlated data can be further parallelized. For transactions operating on the same weakly correlated data, the next transaction can continue execution once the previous transaction is completed but not irreversible. In contrast, strongly correlated data requires waiting until the transaction becomes irreversible before further operations. This classification of data enhances the efficiency of transaction execution in Space Network.

## 6.Smart Contracts

Space Network is a public blockchain network designed for developers, providing special programming primitives and data interaction storage for DApps. These primitives are included within the EVM (Ethereum Virtual Machine). Consequently, in smart contracts, it is possible to access information about data locations, storage nodes, and contributors.

In Space Network, all user data, including real-time transmission and storage, is retained at a high level of privacy and security. Due to the unique characteristics of the IPFS network, even if individual/small-scale servers encounter unforeseen events, the lost data can be fully recovered and stored again through private keys, eliminating any risks. This approach aims to disrupt current privacy and data storage security issues in centralized internet systems.

System Smart Contracts:

```
contract VendingMachine {

	// Declare state variables of the contract
	address public owner;
	mapping (address => uint) public cupcakeBalances;

	// When 'VendingMachine' contract is deployed:
	// 1. set the deploying address as the owner of the contract
	// 2. set the deployed smart contract's cupcake balance to 100
	constructor() {
		owner = msg.sender;
		cupcakeBalances[address(this)] = 100;
	}

	// Allow the owner to increase the smart contract's cupcake balance
	function refill(uint amount) public {
		require(msg.sender == owner, "Only the owner can refill.");
		cupcakeBalances[address(this)] += amount;
	}

	// Allow anyone to purchase cupcakes
	function purchase(uint amount) public payable {
		require(msg.value >= amount * 1 ether, "You must pay at least 1 BOC per cupcake");
		require(cupcakeBalances[address(this)] >= amount, "Not enough cupcakes in stock to complete this purchase");
		cupcakeBalances[address(this)] -= amount;
		cupcakeBalances[msg.sender] += amount;
	}
}
```

## 7.Ecosystem Development

Faced with the challenges of concurrent big data and large-scale storage applications, such as developing decentralized platforms for video, gaming, live streaming, healthcare, health, insurance, education, and other industries accessible to ordinary participants, as well as broader applications in the Internet of Things and metaverse scenarios, my future end-terminal computing devices and IoT devices can all join the SPACE network. Leveraging the technological features of Space Network, effective solutions can be provided. Developers are encouraged to easily develop their own super applications, fulfilling their dreams of changing the world. The public chain will continue to optimize development languages and provide the necessary storage space and network for DApp operation.

## 五 、Space Network Ecological Model

1.Token：BOC

BOC (Binary Options Chain), as the unique designated notarized token on the Space Network, is issued on the Binance Smart Chain (BSC). It will circulate on both the incentive layer and the application layer, constructing the DeFi economic ecosystem through the [SPACE Notarization Law].

1.1 Token Distribution Mechanism

| Distribution and Release Rules for BOC Issuance | |
|---|---|
| Total Issuance: 2 billion tokens | Additional Issuance: None |
| Distribution Mechanism: | Release Rules: |
| 1、Private Placement: 5% | Locked for 12 months, with a monthly release of 1/12. |
| 2、Public Offering: 5% | Locked for 12 months, with a monthly release of 1/12. |
| 2、Foundation: 30% | Locked for 36 months, with a monthly release of 1/36. |
| 3、Technical Team: 10% | Locked for 24 months, with a monthly release of 1/24. |
| 5、Contributor Incentives: 50% | Directly used for BOC ecosystem incentives. |

1.2 Token Burn

1.2.1 Destruction Catalog:

§ Forfeits for violations of the BOC notarization contract;

§ Transaction and transfer fees;

§ Fees for publishing and participating in notarization contracts.

2.Functions of Tokens

2.1 Available for publishing binary smart contracts on the BOC platform. Based on smart contracts, it is a decentralized binary protocol platform where any user can initiate binary protocols on the platform (including binary content, binary amounts, binary definitions).

2.2 Available for secondary market trading. As BOC circulates and binary smart contracts become popular, the value of BOC will gradually rise.

2.3 Security Guarantee: The token network BSC smart chain is always online, and nodes

do not need tokens as collateral. There is also no risk of BSC going offline or disappearing.
2.4 Community Governance: The establishment of Governance Committee nodes and significant changes in decision-making require community voting, and tokens can be used to purchase votes.
2.5 Transfer Payments: Used for gas fees required for on-chain transfers.
2.6 Payment for Other Services: Tokens will also be used for settlements in other applications or services within its ecosystem, and for cross-chain transfer bridges provided by other public chains that offer confidential smart contracts.

## 六、Legal Structure and Risk Warning

1.Legal Structure

The legal entity for the technical development team is SPACE Network Protocol Laboratory. Space Network, as a virtual commodity with practical utility, is not a security nor a speculative investment tool.

Tokens held by the Space Network Foundation will primarily be used for technical development, community building, market promotion, operations, financial auditing, and other purposes.

Space Network may still be subject to inquiries or regulations from regulatory authorities in different countries. In order to comply with local laws and regulations, Space Network may only provide normal services in certain regions or during certain periods.

2.Risk Warning

2.1 Regulatory Risk

Blockchain technology and related operational activities are still in the early stages, and there are no clear legal regulations internationally or domestically in China regarding establishment, information disclosure, and transactions. Moreover, relevant national departments are still in an observation phase without a final conclusion. Changes in the international environment and adjustments in national policies could potentially impact the value and liquidity of Space Network.

2.2 Competition Risk

The blockchain industry has become a popular entrepreneurial direction and is considered by some media and individuals as the second wave of the internet revolution. With the influx of numerous talents and substantial funds, it presents significant development opportunities but also introduces intense competition. While Space Network has assembled an elite team with a comprehensive understanding and determination to address these challenges, we cannot guarantee that the team, ecosystem, and project will necessarily achieve the desired outcomes. Investors should carefully consider this unpredictable risk.

2.3 Talent Attrition Risk

The Space Network project is ready to attract more experienced human resources, technical experts, and marketing professionals. They have confidence and commitment to dedicate their efforts and labor to the project. However, in the future development, it may be inevitable that core management or technical personnel choose to leave. We respect the personal choices of team members, but it is important to emphasize that such departures might have adverse effects on the project's development.

2.4 Hacker Attack Risk

In the development and operation process, Space Network may face malicious attacks from hackers, competitors, and other adversaries. The methods, tactics, and timing of these attacks are unpredictable, and they may result in potential losses for investors.

2.5 Uninsured Loss Risk

Accounts on the blockchain, unlike traditional accounts held with banks or financial institutions, do not have insurance coverage. In the event of any potential risks, there is no institution or individual that will provide insurance or guarantee for the losses incurred by investors on Space Network File net accounts.

2.6 Unknown Risks

In addition to the risks mentioned in the whitepaper, there may be unforeseen or undisclosed risks that the founding team has not anticipated. These risks could emerge suddenly or combine with the mentioned risks in a compound manner. It is hoped that all participants can fully understand the project's situation to make informed investment decisions.

3. Disclaimer

This document is for informational purposes only. The content is provided as a reference and does not constitute any advice, inducement, or invitation for trading stocks or securities of the Space Network project-related companies. This document does not constitute or be understood as providing any buying or selling behavior, nor is it any form of contract or commitment.

Due to unforeseen circumstances, the goals listed in this whitepaper may change. Although the project team will make efforts to achieve project goals, investors purchasing Space Network on the secondary market must bear their own risks. Some documents in this whitepaper may be adjusted with market conditions and technological developments. In such cases, the management team will disclose the adjustments through a new version of the whitepaper.

Space Network explicitly states that it does not assume responsibility for any direct or indirect losses incurred by participants, including:

3.1 Reliance on the content of this document

3.2 Errors, omissions, or inaccuracies in the information in this document

3.3 Any actions resulting from this document

The project team will strive to achieve the project goals listed in the whitepaper. However, due to the existence of force majeure, the team cannot make an absolute commitment to complete realization.

Tokens are incentive tools to achieve project efficiency and are not legal or investment items. Space Network does not represent ownership or control. Controlling Space Network does not mean control over the ecosystem, system, or data. Space Network does not grant any individual or team the power to control and influence decisions regarding the ecosystem, community, system, etc.

## [References]


[1] Juan Benet. IPFS - Content Addressed, Versioned, P2P File Sy st e m. 2014.

[2] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security, pages 598 − 609. Acm, 2007.

[3] Ari Juels and Burton S Kaliski Jr. Pors: Proofs of retrievability for large files. In Proceedings of the 14th ACM conference on Computer and communications secur it y, pages 584 − 597. Acm, 2007.

[4] Hovav Shacham and Brent Waters. Compact proofs of retrievability. In International Conference on the Theory and Application of Cryptol ogy and Information Security, pages 90 − 107. Springer, 2008.

[5] Protocol Labs. Technical Report: Proof-of-Replication. 2017.

[6] Rosario G en nar o, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct ni zk s without pcps. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 626 − 645. Springer, 2013.

[7] Nir Bitansky, Alessandro Chiesa, and Yuval Ishai. Succinct non-interactive arguments via linear interactive proofs. Springer, 2013.

[8] Eli Ben-Sasson, Al e s san d ro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In Advances in Cryptology − CRYPTO 2013, pages 90 − 108. Spr i nge r , 2013.

[9] Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, et al. Computational integrity with a public random string from quasi-linear pcps. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 551 − 579. Springer, 2017.

[10] Henning Pagnia an d Felix C G ¨ artner. On the impossibility of fair exchange without a truste d third party.
Technical report, Technical Re port TUD-BS-1999-02, Darmstadt University of Technology, Department of Computer Science, Darmstadt, Germany, 1999.

[11] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: S cal ab l e o ff -chain instant payments.
2015.

[12] Andrew Miller, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. Sprites: Payment channels that go faster than lightning. arXiv preprint arXiv:1702.05812, 2017.

[13] Protocol Labs. Technical Report: Power Fault Tole ran ce . 2017.

[14] Protocol Labs. Technical Report: Expected Con se ns us . 2017.

[15] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. Proof of acti v ity: E x t en di n g

bitcoin’s
proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Eva lu ati on Review, 42(3) : 34 − 37, 2014.
[16] Iddo Bentov, Rafael Pass, and Elaine Shi . Snow white: Provably secure proofs of st ake. 2016.

[17] Silvio Mic ali . Algorand: The efficient and democratic ledger. arXiv preprint arXiv:1607.01341, 2016.

[18] Vitalik But er i n. Ethereum <https://ethereum.org/>, April 2014. URL https://ethereum.org/.
[19] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
[20] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous pay me nts from bitcoin. In Security and Privacy (SP), 2014 IEEE Symposium on, pages 459 − 474. IEEE, 2014