

Chia as the Blockchain Technology for the Climate Warehouse

October, 2021



Table of Contents

1 Background	7
2 Public vs Private Blockchain	8
2.1 Distributed Ledger Technology	8
2.2 Private Blockchain	8
2.2.1 Enabling Features	8
2.2.2 A Compromise Not Aligned to Principles	8
2.3 Public Blockchain	9
2.3.1 Aligned to Principles	9
2.3.2 Required Features Not Available	9
2.3.3 Database-Style Data Store	9
2.3.4 Chia	9
2.3.5 Key Comparisons: Bitcoin, Ethereum 1.0, Ethereum 2.0 and Chia	10
3 Chia Blockchain	10
3.1 Bram Cohen - Chief Architect of Chia	10
3.2 Public	11
3.2.1 Transparent	11
3.2.2 Inclusive	11
3.2.3 Open Source	11
3.2.4 Sustainable and Secure	11
3.2.5 Autonomous	12
3.2.6 Regulatory Compliance	12
3.2.7 Role of Chia Network	12
3.3 Proof of Space and Time	12
3.3.1 Low Cost Validator Nodes	12
3.3.1.1 Validation of Accessibility	12
3.3.2 Proof of Space	13
3.3.2.1 Proving Space: Bingo Card Analogy	13
3.3.2.2 Proving Space: Operational Efficiency	13
3.3.2.3 Proving Space: e-Waste Avoidance	13

3.3.2.3.1 Not Profitable to Buy New Storage	13
3.3.2.3.2 Overprovisioned Storage	13
3.3.2.3.3 Storage Circular Economy Initiative	13
3.3.2.3.4 Total Storage Used for Chia Blockchain: 42 exabytes	14
3.3.3 Proof of Time	14
3.3.3.1 Proving Time: Verifiable Delay Function (VDF)	14
3.3.3.2 Proving Time: Timelords	14
3.3.3.3 Proving Time: Target Rate	14
3.3.3.4 Proving Time: Timelord Appliance	14
3.3.4 Equitable Distribution of Rewards	14
3.3.4.1 Fractional Rewards: Pooling	14
3.3.4.2 Rewards Exceed Operating Costs	14
3.3.4.3 No Staking and No Penalties	15
3.4 Security	15
3.4.1 Most Decentralized Blockchain in History	15
3.4.2 Attack Resistance: Changing the Rules	15
3.4.3 Attack Resistance: 51% Attack	15
3.5 Ledger Model: UTXO vs Account	15
3.5.1 UTXO is More Efficient	15
3.6 On-Chain Programming: ChiaLisp	16
3.6.1 Functional Programming vs Object-Oriented Programming	16
3.6.2 Turing Complete	16
3.6.3 Performant and Robust Virtual Machine	16
3.6.4 ChiaLisp and the UTXO model	16
3.6.5 Singletons	16
3.7 Chia DataLayer	16
3.7.1 Data Tables	17
3.7.1.1 Data Stored on the Blockchain	17
3.7.1.2 Low Cost to Use	17
3.7.1.3 Subscribing to Data Tables	17

3.7.1.4 Peer to Peer	17
3.7.1.5 Efficient Use of Network Bandwidth	17
3.7.1.6 Data Stored by Subscribing Nodes	17
3.7.1.6.1 Data Lost When No Subscribing Nodes	17
3.7.1.7 Future Capability: Restricted Read Access	17
3.7.1.8 Future Capability: Large Binary Data	17
3.8 Relational Data	18
3.8.1 Primary Keys	18
3.8.1.1 No Duplicate Rows	18
3.8.2 Foreign Keys	18
3.8.3 Enforcing Foreign Key Consistency	18
3.8.4 DataLayer Query Capability	18
3.9 Enabling Data Analytics	18
3.9.1 Notification of Updates	18
3.9.2 Extract, Transform and Load	18
3.9.3 Changing Data	19
3.10 Two-Party Commits	19
3.10.1 Transaction Files	19
3.10.2 Process Flow	19
3.11 Recoverable Authorization	19
3.11.1 Peer-Based Recovery	20
3.11.2 Recovery Process	20
3.11.3 Robust Recovery	20
3.12 Chia Transaction Fees	20
3.12.1 Transactions Have a Cost	20
3.12.1.1 DataLayer Transactions Have Low Cost	21
3.12.2 Blocks Capped at Maximum Cost	21
3.12.3 Priority Equals Fee Divided by Cost	21
3.12.4 Transactions With Low or No Fees	21
3.12.5 No Required Fees, No Minimum Fees	21

3.12.6 Cyclical Fees	21
3.12.7 Blockchain Capacity	21
3.12.8 Future Capacity	22
3.12.9 Future Fees	22
3.12.10 Who Gets the Fees?	22
3.12.11 Transaction Fee Summary	22
3.13 Community	22
3.13.1 Actively Engaging the Public	22
3.13.2 Supporting the Rapidly Expanding Developer Community	22
3.13.2.1 Training and Documentation	23
3.13.2.2 Tools and Support	23
3.13.2.3 Chia Cultivation Grants	23
3.13.2.4 Chia Quarterly Hackathons	23
3.13.2.5 Chia Developer Outreach	23
4 Climate Warehouse on Chia	24
4.1 High-Level Architecture	24
4.1.1 Data Model Implemented on the Chia DataLayer	24
4.1.1.1 Sovereign Data	24
4.1.1.2 Multiple Tables	24
4.1.1.3 Data From Other Participants	24
4.1.1.4 No Shared Tables	24
4.1.1.5 Common Configuration File	24
4.1.2 Chia Node Hosting Climate Warehouse Data	24
4.1.2.1 Low Hardware Requirements	24
4.1.2.2 No Need for Storage for Block Validation	25
4.1.2.3 Local Hosting	25
4.1.3 Climate Warehouse Service Layer	25
4.1.3.1 Standard Interface	25
4.1.3.2 Alternate Interface	25
4.1.3.3 Configuration File Parsing	25

4.1.3.4 Service Layer API	25
4.1.3.4.1 Accessible from Any Modern Programming Language	26
4.1.3.5 Logging	26
4.1.3.6 Open Source	26
4.2 Governance	26
4.2.1 Sovereign Ownership of Data	26
4.2.2 Who Can Participate	26
4.2.3 Support for Subnationals and Metaregistries	26
4.2.4 Data Model Governance	26
4.2.5 Data Model Change Process	26
4.2.6 Change Testing and Validation	26
4.2.7 Double Counting Detection	26
4.2.8 Cancellation Enforcement	27
4.2.9 Support for Coordinated Software Upgrades	27
4.2.10 Future Capability: Funding Models	27
4.2.11 Future Capability: Voting	27
4.2.12 Future Capability: Dispute Resolution	27
4.2.13 Future Capability: Data Aggregation and Presentation	27
5 Auxiliary Application	28
5.1 Portable, Electron-Based Application	28
5.2 Familiar Interface	28
5.3 No Servers	28
5.4 Manual Entry and Spreadsheet Upload	28
5.5 Export	28
5.6 Support for 2-Party Commit Transfers	28
5.7 Installer and Uninstaller	28
5.8 Open Source	28

1 Background

The Climate Warehouse will provide the global market infrastructure that can mobilize climate action to achieve the Paris Agreement's objectives by enhancing transparency and environmental integrity of carbon credit transactions and international carbon markets.¹

The World Bank provided context for the Climate Warehouse in 2019 [here](#):

Context

The Paris Agreement introduced a bottom-up approach for addressing climate change by enabling countries to pledge individual commitments through nationally determined contributions (NDCs). Furthermore, Article 6 of the Paris Agreement recognizes that Parties may engage in bilateral cooperative approaches, including through the use of internationally transferred mitigation outcomes (ITMOs), to achieve their NDCs.

Heterogeneous climate markets may have different governance systems and technological approaches. Information about mitigation outcomes (MOs) or emission reductions is currently collected in a variety of repositories, including spreadsheets and registries, with different levels of information. The differences in these processes may constrain market integration and add to the complexity of tracking and recording transactions.

Against this backdrop, there is a need to create a new architecture to support transparency and enhance the tradability of climate assets across jurisdictions while ensuring the integrity of trades. The Kyoto Protocol utilized an International Transaction Log (ITL), operated by the United Nations Framework Convention on Climate Change (UNFCCC), to facilitate communication between registries and maintain a transaction log to ensure accurate accounting and verification of transactions proposed by connected registries. However, under the Paris Agreement, which may rely on a decentralized approach to markets under Article 6.2, climate negotiators are still determining whether a centralized infrastructure should continue, the functions it could perform, and to which market mechanisms or transactions it would apply. Consistent with the bottom-up ethos of the Paris Agreement, there is value in demonstrating an approach to link registry systems in a peer-to-peer arrangement.

Climate Warehouse Vision

The World Bank's Carbon Markets and Innovation team (CMI) has a mandate to pilot options to contribute to the understanding of the opportunities of Article 6 and build client capacities to engage in the next generation of climate markets.

As part of this mandate, CMI is exploring a Climate Warehouse ecosystem to demonstrate a decentralized information technology approach to connect climate market systems. In the Climate Warehouse ecosystem, a meta-registry system would connect to country, regional, and institutional databases and registries to surface publicly-available information on MOs and record status changes to provide information on how MOs are used. The objective of this meta-registry would be to reduce double counting risks¹ by enhancing transparency and trust among market participants and tracking MOs across jurisdictions.

¹ From *Briefing Paper: The Governance and Financing of an Operational Climate Warehouse*, Sept 8, 2021

Over the past three years, Carbon Markets and Innovation Team and the World Bank's Technology Innovation / Blockchain Lab have undertaken an extensive design study, including two full simulations, to assess the technology platform with the necessary functionality that can best achieve the objectives while aligned with the guiding principles of the Climate Warehouse.

Leveraging experience gained through this process, the Chia Blockchain has emerged as an open-source public blockchain that has the ability to host a permissioned, distributed database that runs on inexpensive non-proprietary hardware. The use of the Chia blockchain platform allows for the complete Climate Warehouse application, including data nodes, APIs, and auxiliary applications to be easily implemented and governed as secure, open-source, and inclusive technology.

This white paper is intended to describe the Chia technology in detail as it applies to the implementation of the Climate Warehouse. It was created by a team of leading cryptographers and developers, some of whom have been involved in peer-to-peer protocols for two decades, to deliver functionality, security and sustainability that was previously considered impossible on a public blockchain.

2 Public vs Private Blockchain

The most fundamental technology selection for the Climate Warehouse is the underlying data store. Decentralized databases exist in three different forms today:

- Distributed Ledger Technology (DLT)
- Private Blockchain
- Public Blockchain

2.1 Distributed Ledger Technology

DLT is a type of private distributed database that does not create a tamper proof chain with the immutability guarantees of a blockchain. Immutability is a key requirement for the Climate Warehouse to secure a sequential series of events that are fully transparent.

2.2 Private Blockchain

A private blockchain is one where the participants each host a validator node, which is a computer running blockchain-specific software to validate the blockchain and to extend it with new data. They tend to be very feature-rich, performant and have very little climate impact.

2.2.1 Enabling Features

Previous simulations of the Climate Warehouse used private blockchains because they provided the needed features unavailable in DLT or public blockchains available at the time:

- They support powerful database features
- They are immutable
- They have predictable costs
- They have low environmental impact

2.2.2 A Compromise Not Aligned to Principles

Private blockchain technologies did meet most of the functional needs of the Climate Warehouse application, but did not fit well with the goals of the World Bank in this setting. One key feature of all private blockchains is permissioned access. Only those participating in the blockchain have direct access

to it. For everyone else, the system is essentially closed and inaccessible. Members can each present the data externally the way they see fit, but if the data that two participants present appears to conflict, non-participants have no way to study the underlying data to get transparency.

Private blockchains also have an administrator role held by at least one participant that gives that participant greater control over the system and the other participants, which is undesirable in the context of the peer-to-peer, decentralized ethos of the Paris Agreement. The security and immutability of a blockchain is directly related to the number of validator nodes working to secure it. With nodes operated only by participants, private blockchains are also much less secure.

2.3 Public Blockchain

Public blockchain technology uses a worldwide network of thousands of computers securing the network by validating every transaction.

2.3.1 Aligned to Principles

Public blockchains are well aligned with the larger goals of the World Bank for the project:

- They are highly decentralized
- They are very secure
- They are immutable
- They are inclusive - everyone can participate
- They are transparent - everyone can see every transaction

2.3.2 Required Features Not Available

At the time of Climate Warehouse simulations 1 and 2, there was no public blockchain that supported the needed features to host the Climate Warehouse. Specifically:

- Native data store for structured data with permissioned access
- Low expected transaction costs
- Low environmental impact

Without these features, it was not feasible to attempt a simulation on a public blockchain.

2.3.3 Database-Style Data Store

All programmable public blockchains have some means of storing data, but none provide a full relational database style data store. Also, there are some third party solutions for associating a permissioned database to a blockchain to enable verification. But none of those enable that data to be publicly available through the blockchain, and none allow that data to participate in blockchain transactions. Without this capability, these blockchains cannot store the Climate Warehouse data directly.

2.3.4 Chia

Chia is an innovative blockchain that provides both the needed functionality and the alignment to World Bank principles that is ideal for the Climate Warehouse. This paper will describe that alignment in detail.

2.3.5 Key Comparisons: Bitcoin, Ethereum 1.0, Ethereum 2.0 and Chia

	Private Blockchain	Public Proof of Work: Bitcoin, Ethereum 1.0	Public Proof of Stake: Ethereum 2.0	Public Proof of Space and Time: Chia
Decentralization	Low	High	Medium	Highest (50x Ethereum 1.0)
Security	Relatively easily subverted by a bad actor with permissioned access	Secure	Fewer actual validator nodes Enables certain types of attacks	Most secure
Inclusivity	Limited to permissioned users	Public access Significant ongoing investment from validators	Public access Significant investment required to be a validator	Public access Very low investment to participate in validation
Transparency	Only accessible by permissioned users	Transparent	Transparent	Transparent
Native Data Storage	Yes	No	No	Yes
Transaction Costs	Low	High	High	Expected to Remain Low
Environmental Impact	Minimal	Very High	Low	Low

3 Chia Blockchain

Chia is an innovative public blockchain technology designed to be both sustainable and secure with functionality not otherwise available on a public blockchain.

3.1 Bram Cohen - Chief Architect of Chia

Chia Network was established in 2017 by peer-to-peer networking pioneer Bram Cohen. Before Chia, he founded BitTorrent, the hugely influential decentralized file-sharing protocol. In 2009, 43% to 70% of the entire internet's global traffic was attributed to Bittorrent, and up to 19% of global internet upstream traffic at present day. Before BitTorrent, Bram worked at MojoNation, one of the earliest attempts at digital currency.

Cohen's experience building that vast global network influenced how he created Chia with "last mover advantage", allowing him to design it to be both sustainable and secure with functionality not otherwise available on a public blockchain.

3.2 Public

There are two main types of blockchains: public and private. A public blockchain is secured by thousands of validators all over the world and is transparent and accessible worldwide. Private blockchains have very few validators and typically provide additional features such as built-in databases. Chia is the world's most decentralized and secure public blockchain, and it also has low fees and supports features previously only available on private blockchains.

3.2.1 Transparent

In a public blockchain, anyone can run the appropriate software and get a complete, verifiable, unencrypted copy of all of the data on the blockchain. It is completely transparent and open to independent review. In a private blockchain, access to the blockchain must be restricted, and non-members must depend on one of the members to make the data available. With a private blockchain, non-members must trust members and assume that the data they receive is complete and unaltered.

3.2.2 Inclusive

Public blockchains are open to participation by all and are fully transparent, open to inspection by all. A private blockchain is centralized in that it requires an administrator that restricts who can participate and assigns permissions to each participant. In a private blockchain, participants cannot securely verify the permissions given to other participants in order to confirm that no one has an advantage. In a public blockchain, there is no such authority or permissions.

3.2.3 Open Source

Nearly all public blockchains use freely available, open-source software. Use of the software does not require a relationship with any commercial entity, even the developer of the software, so there is no risk that such an entity could start demanding high fees for use of the software. As open source software, even if the entity that created the software were to be dissolved, another entity could take up ongoing maintenance of the code. Several major private blockchains are open-source only for purposes of allowing review, but still require ongoing costs to use.

There are several open source licenses, and Chia Network uses the Apache License 2.0. Additionally, all of Chia's patents are immediately given to the community under the Crypto Open Patent Alliance (<https://www.opencrypto.org/>). As open source software, there is no risk that any entity could start demanding fees for the use of the Chia blockchain software.

3.2.4 Sustainable and Secure

Bitcoin introduced the first useful application of Proof of Work consensus, where computers race to solve cryptographic puzzles to win the right to add blocks to the blockchain and earn the associated rewards. This incentivizes people to use ever-faster computers and consume vast amounts of energy to compete. While it is very secure, it is unsustainable due to the very high energy consumption, which will only increase with increased adoption.

Proof of Stake is a consensus mechanism that requires people to stake a certain amount of currency to earn the right to add blocks and accept the associated rewards. This is exclusionary and can quickly lead to centralization and reduced security when a small number of individuals with large stakes emerge. This has been proposed by several major cryptocurrency stakeholders, and it clearly benefits larger stakeholders who will maintain more control and collect an outsized share of mining / validation rewards.

Chia uses an innovative Proof of Space and Time consensus that is inclusive, equitable, secure, and intrinsically sustainable.

3.2.5 Autonomous

The Chia blockchain runs autonomously. No company or entity, including Chia Network itself, has control over the blockchain. At a technical level, it is not possible for Chia Network or anyone else to exclude participants, revert or override transactions or in any other way assert undue control over the Chia blockchain.

3.2.6 Regulatory Compliance

In order to assure long-term regulatory compliance, Chia Network intends to become a publicly traded company on an accelerated timeline with all of the board and shareholder oversight that entails. Chia Network has engaged with a leading law firm to manage this process, and works closely with regulatory experts to ensure the corporate structure, governance and internal controls will pass an audit smoothly. Chia Network has never sold XCH, the currency associated with the Chia blockchain, ensuring that the token cannot be considered a security in the company.

3.2.7 Role of Chia Network

Chia Network is the company responsible for developing the Chia blockchain software. Additionally, it also has a professional services organization that assists governments, NGOs and private companies in building enterprise-grade solutions on the Chia blockchain. It is in this capacity that Chia Network is helping to develop the Climate Warehouse. Chia's services for the Climate Warehouse are being offered free of charge and on a non-exclusive basis.

The governance associated with public ownership will ensure Chia Network cannot use its role as the developers of the Chia software to assert undue control over the Chia blockchain. Even if Chia Network were to publish a version of the software that asserted or enabled it to have such control, that version would need to be adopted by at least half the node operators to become effective. Chia is a truly public blockchain, operated by the global public, not by Chia Network.

3.3 Proof of Space and Time

The Chia blockchain uses an innovative consensus algorithm called Proof of Space and Time that avoids the energy waste of Proof of Work and is more secure and inclusive than Proof of Stake. It uses two types of proofs: proof of space and proof of time. These proofs alternate one after the other as the Chia blockchain grows.

3.3.1 Low Cost Validator Nodes

Like all blockchains, validation of the blockchain uses a network of validator nodes - computers running blockchain-specific software to validate the blockchain and to extend it with new data. The minimum-spec computer required to run a Chia validator node is a Raspberry Pi 4, which can be

purchased new for less than 100 USD. Any computer using an Intel-compatible 64-bit processor, including most PCs built in the last 13 years, is sufficient.

3.3.1.1 Validation of Accessibility

Currently, there are over 300,000 Chia validator nodes running all over the world. The sheer number of nodes is proof that Chia software is accessible to all, easy to use and inclusive.

3.3.2 Proof of Space

In Proof of Work, validator nodes earn the right to add blocks to the blockchain by proving that they are doing a certain amount of ongoing work to solve cryptographic puzzles. In Proof of Stake, nodes must prove a financial stake in the blockchain. Chia validator nodes use a proof of storage space allocated to the blockchain to earn the right to extend the chain.

3.3.2.1 Proving Space: Bingo Card Analogy

To prove space allocated to the blockchain, a Chia validator node first fills the available space with the outputs of a complex algorithm on a series of random inputs. Those outputs are analogous to bingo cards - the validator node that has the closest card to the one required to add the next block wins the opportunity to do so.

3.3.2.2 Proving Space: Operational Efficiency

There is very little energy used in the ongoing operation of a Chia validator node. Approximately 4,600 blocks per day are added to the chain. For every 100GB of space allocated to the blockchain, a Chia validator node will only attempt to participate in approximately 9 blocks, and will issue only 7 disk read requests for each block it attempts.

As a result of this low energy use per node, the Chia blockchain uses very little energy globally. Chia uses less than 0.15% of the energy of Bitcoin, despite having over 300,000 nodes compared to Bitcoin's 65,000 nodes. Chia also uses less than 0.3% of the energy of Ethereum 1, which has approximately 5,500 nodes. More information can be found at <https://chiapower.org>.

3.3.2.3 Proving Space: e-Waste Avoidance

It is rarely profitable to purchase new computers or storage devices to operate a Chia validator node. Like all public blockchains, the operator of the validator node that successfully adds a node block to the blockchain earns a reward. With Chia, the likelihood of earning that reward is proportional to the validator node's allocated space as a percentage of the total space allocated by all validator nodes.

3.3.2.3.1 Not Profitable to Buy New Storage

After the launch of the Chia blockchain, the total space allocated by validator nodes grew quickly until it reached an equilibrium point such that it would take approximately a year for blockchain rewards to pay for the purchase price of the cheapest new storage - effectively stopping node operators from investing in new storage just for the Chia blockchain.

3.3.2.3.2 Overprovisioned Storage

Many people and organizations have more storage than they need. As awareness of Chia grows, some of that storage will be allocated to Chia validator nodes. This already-existing storage represents zero marginal cost for the node operator, and any rewards earned will be profit. As this storage gets added to the total allocated to Chia blockchain, it will further depress the returns available from buying new storage for Chia validator nodes.

3.3.2.3.3 Storage Circular Economy Initiative

Chia Network, Inc is working with all three major hard drive manufacturers and several major cloud service providers on a secure circular economy initiative. Currently, cloud service providers decommission hard drives after 3 to 5 years of use. Today, these hard drives are shredded to eliminate concerns over data privacy. This initiative aims to securely erase, repurpose and ultimately recycle these 20 million decommissioned hard drives per year.

3.3.2.3.4 Total Storage Used for Chia Blockchain: 42 exabytes

As of September 2021, the total storage allocated worldwide to the Chia blockchain by all validator nodes is 42 exabytes. For comparison, the largest hard drives commonly installed in new personal computers can store 1 terabyte. 42 exabytes is 42,000,000 terabytes.

3.3.3 Proof of Time

As the proof of space is so efficient, another mechanism must be used to limit the rate at which blocks can be added to the Chia blockchain to ensure the security of the Nakamoto consensus algorithm.

3.3.3.1 Proving Time: Verifiable Delay Function (VDF)

To prove that time has passed, Chia has created a verifiable delay function. This is a mathematical function that is very hard to compute but easy to verify.

3.3.3.2 Proving Time: Timelords

The Chia network uses community-operated “timelord” computers to run the verifiable delay functions to confirm each block added to the Chia blockchain by a validator node. For any block, the timelord that completes the confirmation VDF fastest signs the block. There are no rewards for running a timelord, so the number of timelords running these functions on an ongoing basis is small.

3.3.3.3 Proving Time: Target Rate

The verifiable delay function can be made harder or easier based on a parameter. That parameter is periodically adjusted so that the blockchain consistently runs at the expected number of blocks per day.

3.3.3.4 Proving Time: Timelord Appliance

Chia Network, Inc is working with a third party to create a low-cost ASIC-based appliance that will run the verifiable delay function marginally faster than the current fastest general-purpose computers. This enables community members that want to participate in the Proof of Time to do so effectively at reasonable cost.

3.3.4 Equitable Distribution of Rewards

Like all blockchains, the rewards for adding blocks to the chain are the incentives that support the validator node operators worldwide. As the total storage space allocated to Chia increases, the frequency with which any particular node operator gets rewards decreases.

3.3.4.1 Fractional Rewards: Pooling

To be more inclusive of community members that do not have a lot of storage available, Chia has developed a *secure pooling protocol* that enables even very small validator node operators to receive rewards on a regular, even daily, basis. These rewards are smaller, in proportion to the space that the operator provides, but received regularly. Importantly, members that choose to participate in a pool still participate as full peers in the blockchain, running the same full validator node as larger members.

3.3.4.2 Rewards Exceed Operating Costs

Once set up, the validator node takes very little CPU and very little to no ongoing cost for storage. Currently, 10 terabytes of storage earns about USD \$12 per month, even at the current relatively low native currency price. Even long after it stops making sense to buy new storage for running a Chia validator node, it will still make sense to continue to operate overprovisioned or otherwise unused space for Chia validation.

3.3.4.3 No Staking and No Penalties

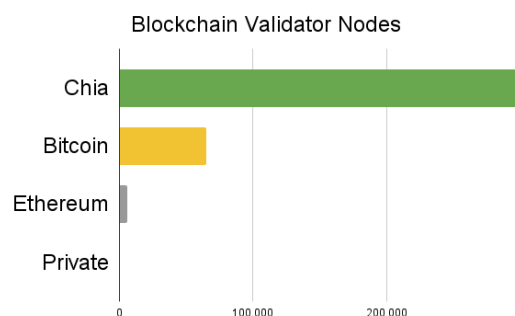
Participation in the Chia blockchain does not require any currency to be locked up, or “staked”, as in Proof of Stake based blockchains. Staking also comes with penalties that can be assessed that will reduce or eliminate the participant’s staked currency. Staking and the risk of penalties, even with very low minimum stake amounts, limits the ability of some users to participate.

3.4 Security

The Chia blockchain is a full Nakamoto consensus blockchain, secured in much the same way Bitcoin is secured, just with a different proof mechanism: proof of space and time instead of proof of work.

3.4.1 Most Decentralized Blockchain in History

The Chia blockchain has over 300,000 nodes, all participating as global peers. For comparison, Bitcoin had approximately 200,000 nodes at its peak, and now has 65,000. Ethereum currently has approximately 5,500.



3.4.2 Attack Resistance: Changing the Rules

To change the rules of a robust, Nakamoto-consensus blockchain requires 51% of the nodes to be corrupted. The Chia network has over 300,000 nodes, so an attacker would have to hack or otherwise subvert over 150,000 nodes.

3.4.3 Attack Resistance: 51% Attack

In a Nakamoto consensus blockchain, successful attacks require 51% of the resources allocated to the blockchain: in proof of work, that is 51% of the total ongoing work (“hashrate”) and in proof of space and time, that is 51% of the total allocated storage. To control more than half of the storage allocated to the Chia blockchain, an attacker would need to allocate more than the total allocated by honest participants: currently 42 exabytes.

3.5 Ledger Model: UTXO vs Account

The Account Model is used in Ethereum and most Proof of Stake blockchains. It works like normal double-entry accounting: each transaction involves debiting one account and crediting another. The *unspent transaction outputs* (UTXO) model was invented for Bitcoin and is more efficient for use on blockchain: value is represented in data records called *coins* in Chia or UTXO in Bitcoin. Each transaction involves canceling coin(s) of a certain value and creating new coin(s) of equal value that are available to the other user(s). To protect the immutability of the blockchain, no coin is ever changed once created.

3.5.1 UTXO is More Efficient

The UTXO Model is much more efficient in space and performance for validation on the blockchain than the account model. It is part of the reason Chia is able to run on lower-spec computers.

3.6 On-Chain Programming: ChiaLisp

Ethereum introduced Smart Contracts, the capability for the blockchain to execute code. For example, a Smart Contract might provide for a secure, auditable auction, such that not even a corrupt auctioneer can unfairly affect the execution or outcome of the auction. Ethereum contracts are written in Solidity, an object-oriented language whose design was most influenced by C++.

3.6.1 Functional Programming vs Object-Oriented Programming

Most languages today are object-oriented languages because that style of language is most appropriate for large applications. They facilitate the organization of functionality into units called *objects* that programmers find natural to use. However, the complexity in the way the objects interact makes it very difficult to identify all possible interactions and confirm correctness in all cases.

ChiaLisp is a type of language called a functional language and it works very differently. Code in a functional language is *stateless*: it only processes the data it is given, and does not have access to (and cannot be affected by) any other code or data. That feature eliminates whole categories of bugs and makes it much easier to confidently assess the correctness of a program. Functional programming is becoming increasingly popular in the financial services industry for that reason.

3.6.2 Turing Complete

Computer scientists have a tool to assess limitations on the functionality that can be implemented in a particular language, and a language with no such limitations is said to be “Turing complete”. ChiaLisp meets that standard.

3.6.3 Performant and Robust Virtual Machine

ChiaLisp code cannot be compiled and run directly. Instead, a part of the Chia validator node software called the ChiaLisp Virtual Machine (CLVM) runs the ChiaLisp code. CLVM is written in Rust, a modern, high-performance programming language with strong guardrails to help prevent bugs.

3.6.4 ChiaLisp and the UTXO model

Lisp is unique even among functional languages in that it lends itself well to compression. It is so efficient that in Chia every coin record has a ChiaLisp program that determines how it can be spent. Each coin can also store a small amount of information. By far the most common stored data is the cryptographic public key for which a user must demonstrate ownership of the corresponding private key to spend the coin.

3.6.5 Singletons

One common ChiaLisp program is a singleton - a coin that can only be spent to recreate a copy of itself. Once created, only one unspent instance of a singleton can exist. This is the basic structure used for NFTs (“non-fungible tokens”), which have become popular recently as a means to represent ownership of unique assets, such as art images. In the context of the Climate Warehouse, this is the structure that enables the creation of the Chia DataLayer, described below.

3.7 Chia DataLayer

Chia supports a simple, relational database called the Chia DataLayer. Like the transactions on the Chia public blockchain, the data stored in the DataLayer is secured by the entire 300,000-node worldwide network of validator nodes.

3.7.1 Data Tables

Each table of data on the Chia blockchain is represented by a singleton coin. Any blockchain node that subscribes to that table also stores the complete table data.

3.7.1.1 Data Stored on the Blockchain

The table singleton stores three pieces of information:

- An identifier that never changes
- The secure hash (using the SHA-256 algorithm) of the data currently stored in that table
- A list of the users that have write access to change the data in the table

3.7.1.2 Low Cost to Use

The table singleton is a very lightweight ChiaLisp program and, barring an unreasonably large list of users with write access, takes very little space on the blockchain. The only time the singleton is “spent” with an on-chain transaction is when a collection of changes to that table is committed. The size of the singleton coin on the blockchain does not change regardless of the amount of data stored in the data table it represents. Thus, the transaction fees associated with using a DataLayer table are kept very low.

3.7.1.3 Subscribing to Data Tables

Each validator node operator has the option to “subscribe” to DataLayer tables. Upon subscribing to a table, that node will download a copy of the table and use the hash stored in the corresponding singleton on the blockchain to confirm the received data is correct. Whenever the singleton is updated, all of the nodes that subscribe to that table will get the updated data and will use the updated hash stored in the singleton to confirm they each have the correct data.

3.7.1.4 Peer to Peer

The nodes subscribing to a DataLayer table create a peer-to-peer network, propagating data updates among themselves.

3.7.1.5 Efficient Use of Network Bandwidth

Each node only downloads an update to the data in a table from its peers once, and the protocol ensures that no one node carries a disproportionate share of the uploads.

3.7.1.6 Data Stored by Subscribing Nodes

The data in a DataLayer table is only stored by those nodes that subscribe to it. There is no storage required for that data on any node that does not subscribe to the data.

3.7.1.6.1 Data Lost When No Subscribing Nodes

If at any point there are no nodes subscribing to the data for a data table singleton, that data will be lost unless it is otherwise stored outside of the Chia DataLayer.

3.7.1.7 Future Capability: Restricted Read Access

In a future version of DataLayer, Chia will support limiting read access to data in DataLayer tables. This will allow for certain data to be only shared with trusted third parties, but not with the public at large.

3.7.1.8 Future Capability: Large Binary Data

In a future version of DataLayer, Chia will support binary large object (BLOB) data in DataLayer tables. This can include PDFs, satellite imagery, etc.

3.8 Relational Data

There are no restrictions on the data stored in each row of a DataLayer data table. By convention, the list of elements in each row is logically the same as the lists of elements in every other row in that table. This allows for the data to be treated as tabular data, with rows and columns.

3.8.1 Primary Keys

In database terms, the primary key for a table is a column that is unique for every row in the table. In the Chia DataLayer, every row has a hash value guaranteed to be unique that is the default primary key.

3.8.1.1 No Duplicate Rows

Because the Chia DataLayer stores rows by hash value, it cannot store multiple, duplicate copies of a row. Every row must be unique in some way.

3.8.2 Foreign Keys

A row in one table can reference a row in another table by the primary key of the referenced row. This reference is called a foreign key. In Chia DataLayer, an element in a row in one table that stores the hash of a row in another table effectively implements a foreign key relationship between the rows.

3.8.3 Enforcing Foreign Key Consistency

The Chia DataLayer is not currently capable of enforcing foreign key relationships between tables.

3.8.4 DataLayer Query Capability

At this time, the Chia DataLayer does not support SQL-style structured queries that join multiple tables through foreign key relationships. DataLayer tables support the following queries:

- Query for an individual row by the row hash value
- Query to get all rows in the table
- Query for the inserted and deleted rows associated with a specific commit by commit number
- Query to get the current commit number

3.9 Enabling Data Analytics

There are many tools available for creating rich dashboards, reports and summary data that depend on the ability to perform sophisticated queries that the Chia DataLayer does not support. To support this functionality, the Chia validator nodes software provides a local DataLayer API that enables external data tools to maintain an up-to-date, read-only view of the data. These tools can then provide the rich data experience that users demand.

3.9.1 Notification of Updates

Using the DataLayer API, a process can request notification when a DataLayer table has changed. In response to that notification, the process can then request from the DataLayer API the collection of inserted and deleted rows associated with that change.

3.9.2 Extract, Transform and Load

A common database process is called Extract, Transform and Load (ETL), and is the process of extracting data from one system, potentially transforming it in some way, and loading it into another database. Using the DataLayer notification mechanism, a process can dynamically replicate data stored in the Chia DataLayer into any data analytics, reporting or visualization tool.

3.9.3 Changing Data

Changes to data rows stored in Chia DataLayer must be submitted directly to the DataLayer APIs. When these changes are confirmed on the blockchain, all nodes including the one that submitted the change will be notified.

3.10 Two-Party Commits

Updates to DataLayer data by two parties can be committed to the blockchain simultaneously such that the change only occurs if both parties agree to the change. This can be used to ensure that neither party commits a change to its own tables without a corresponding agreed change to the other party's tables. This process also ensures that the blockchain can show that both parties agreed to the change, and the identities that signed both sides of the transaction can be identified.

3.10.1 Transaction Files

A transaction file contains a signed commitment from one party and a demand of the other party. If agreed, the other party signs the transaction file and submits it to the blockchain. A transaction file can include any commitment and demand that can be represented on the blockchain. In the context of DataLayer, the commitment and demand can be corresponding database updates to data tables owned by two parties.

3.10.2 Process Flow

To implement a two-party commit:

- Party A and Party B come to an agreement off-line
- Party A creates the necessary data table updates for its own tables and that of Party B to represent the agreement
- Party A creates a transaction file containing the necessary DataLayer singleton updates and signs it, committing to making the changes to its own tables if the corresponding changes are made to Party B's tables.
- Party A sends the transaction file and data table updates to Party B.
- Party B confirms the data table updates are as agreed and match the singleton updates in the transaction file.
- If Party B agrees that the transaction file is correct, Party B signs it and submits it to the blockchain.



- When the transaction is confirmed, both parties update their local data tables.
- If needed, Party B could have declined to accept the transaction file, and no changes would be committed to the blockchain.

3.11 Recoverable Authorization

The authorization used to provide write access to DataLayer tables is recoverable in case the underlying keys are lost or compromised. The authorization is associated with a simple Chia digital identity, which can be asserted using a key. Using the recovery process, a new key can be associated with that identity.

3.11.1 Peer-Based Recovery

The recovery process allows a collection of peers to attest that a recovery operation is valid. Any number of peers can be identified as trusted to attest to the recovery, and at recovery time, only a subset of those peers is required. The collection of peers and the size of the subset of the peers needed to perform the recovery must be specified in advance, before an event occurs that requires a recovery.

3.11.2 Recovery Process

After the Chia digital identity is created, the owner should prepare for recovery, in case it is needed in the future. To prepare:

- The user selects some number of other Chia digital identities that are trusted to attest to the recovery of their digital identity. The user also selects how many of those peers that are required to attest to the restoration.
- The user uses the Chia wallet software to create a backup file of the digital identity.
 - This file does not have enough information for an attacker to identify the trusted peers.
- The user saves this backup file somewhere safe.

Once it is discovered that the keys used for that digital identity are lost or compromised, the user proceeds with the restoration process:

- The user creates a new private key.
- The user uses the Chia wallet software to start the restoration process by loading the backup file.
- The user will be presented with some information from the backup file, which they send to each of the attesting peers.
- The peers each use the Chia wallet software to create an attestation file with their own Chia digital identity, based on the information provided.
- The peers each save their attestation files and send them to the user.
- The user uses the Chia wallet software to load all of the attestation files.
- When enough attestation files are loaded, the Chia digital identity will be transferred to the new private key.

3.11.3 Robust Recovery

The recovery process does not depend on the keys of the peers, but their Chia digital identities. Thus, when one of the peers goes through the recovery process, their recovered digital identity can still be used to create the needed attestation files for the user, even though the underlying keys have changed.

3.12 Chia Transaction Fees

All public blockchains have a limited rate at which they can process transactions. It is a simple consequence of having fixed-size blocks at relatively fixed time intervals. At the same time, anyone can submit a transaction to the blockchain at any time. How does the blockchain prioritize which transactions should be included in a block when there are too many transactions to fit in it?

3.12.1 Transactions Have a Cost

On the Chia blockchain, there is no calculation for the fee required for a transaction. Instead, there is a calculation for the *cost* to the blockchain to process the transaction, both in terms of processing complexity and storage required. This cost for a transaction can be estimated prior to submitting the transaction. This cost is a relative measure used to compare two transactions to determine which demands more of the blockchain's resources.

3.12.1.1 DataLayer Transactions Have Low Cost

It is worth noting here that DataLayer transactions have very low cost: the ChiaLisp programs are small and there is very little data actually stored on the blockchain. The transaction cost is the same regardless of the amount of data stored in a DataLayer table. Specifically for the Climate Warehouse, updates that participants make to the data they store in the Climate Warehouse will not incur any extra fee based on the volume of data stored.

3.12.2 Blocks Capped at Maximum Cost

Every block has a maximum total cost - the maximum resources that can be spent to process that block. When the total cost of the pending transactions is less than the maximum cost allowed per block, the blockchain will usually include all of the pending transactions, regardless of fee paid. When blocks are below capacity, it does not make sense to offer a fee when submitting a transaction to the blockchain.

3.12.3 Priority Equals Fee Divided by Cost

When the total cost of the pending transactions exceeds the maximum cost for a block, the validator node must decide which transactions to include. By default, the validator node will select transactions to earn the maximum available fee. It does this by prioritizing the most profitable transactions - those that pay the highest fee for the lowest cost to the blockchain. Those transactions that do not make it into the current block will be considered for the next.

3.12.4 Transactions With Low or No Fees

So long as the blockchain is below capacity, transactions submitted with no fee will be confirmed just as quickly as transactions with high fees. Even as the blockchain begins to approach capacity, the transactions with lower priority (fee divided by cost) will simply get delayed by a few blocks, but will still be completed.

3.12.5 No Required Fees, No Minimum Fees

The fee paid with each transaction is entirely up to the submitter of the transaction based on the relative priority they want to assign to their transaction. Only in the case that the blockchain is consistently full over an extended period is it possible for a transaction to be abandoned.

3.12.6 Cyclical Fees

Fees in Bitcoin and Ethereum are cyclical - rising and falling over the course of each day based on demand. To minimize fees when they are required, Climate Warehouse participants can delay submitting data updates until a low point in the cycle.

3.12.7 Blockchain Capacity

Chia has about 20% greater throughput than Ethereum. As of September 2021, Ethereum is currently at capacity and processing about 1.2M transactions per day - and every transaction requires a fee or it will be abandoned. Chia is currently processing about 200K transactions per day. Chia blocks are currently at about 10-15% capacity, with some blocks getting as much as 30% full. Paying a fee does not affect the speed of confirmation of transactions on Chia right now.

3.12.8 Future Capacity

Chia is actively planning for a Lightning-style layer-2 protocol to dramatically accelerate transactions. This type of protocol executes a lot of transactions off chain and only submits to the main blockchain (layer-1) the net of those transactions. The Lightning protocol on Bitcoin has proven very effective.

Enabling this protocol in Chia is on the roadmap for delivery in 2H2022. Using the UTXO model greatly simplifies the implementation of this type of layer-2 protocol. All smart contracts written in ChiaLisp will continue to work on this layer-2 as they do on Chia today. When that becomes available, the effective capacity of the Chia blockchain will be much greater, ensuring that fees remain low.

3.12.9 Future Fees

It is difficult to estimate when the Chia blockchain will start to hit capacity and has the potential to begin to abandon some transactions. Only then will it start to require fees. It is especially difficult to estimate given the planned layer-2 protocol. It depends on the rate of adoption of Chia.

3.12.10 Who Gets the Fees?

The operators of the 300,000+ validator nodes each get the fees associated with the transactions in the blocks that they successfully add to the blockchain. As the Chia blockchain starts to approach capacity, the additional revenue stream from fees will continue to incentivize people to operate validator nodes. Node operators that choose to join a pool keep the fees for the blocks they validate and do not share those fees with the pool.

3.12.11 Transaction Fee Summary

The bottom line is that there are no fees today, and Chia Network does not expect significant fees to be required for a long time to come. Chia Network has no control over the fees paid nor when they will be required.

3.13 Community

Chia Network, the company, has an active and dedicated community. Bram Cohen has developed a large following and Chia has been much anticipated and a high profile initiative for years before it was launched. Chia has embraced this active role and since the beginning of the company, it has hosted a community of interested individuals from all over the world in the Keybase platform. The community extends beyond “farmers” to technical gurus and a rapidly expanding development community that recognizes the advantages of Chia’s security and highly functional ChiaLisp programming language.

3.13.1 Actively Engaging the Public

In the Keybase platform, Chia leadership and developers are frequently available there to answer questions, comment on recent news, etc. The community has remained positive, supportive and engaged, and includes nearly 20,000 members. Several members of that community have been hired into the company. Chia also regularly hosts online video AMAs (“Ask Me Anything”) to make sure those interested in Chia are well informed and have the opportunity to ask questions. The senior leadership team including Bram Cohen have also made themselves available for interviews with the media outlets.

3.13.2 Supporting the Rapidly Expanding Developer Community

Chia Network is supporting their active developer community in a number of ways:

3.13.2.1 Training and Documentation

Chia Network has made a significant effort to make available training materials and documentation to enable developers on the journey to proficiency with Chia and ChiaLisp. There are hours of videos, multiple tutorials, and complete documentation available online.

3.13.2.2 Tools and Support

Chia Network is making ongoing, continuous investments into providing robust, powerful and intuitive tools to make developing in ChiaLisp easy. The community has responded in kind: there have been an explosion of tools created outside of Chia Network that include everything from No-Code tools for auto-generating ChiaLisp code to complete development environments and plugins for several popular commercial Integrated Design Environments (IDEs).

In addition, a team of Chia’s technical experts are available almost 24/7 on Keybase channels. Legitimate questions or support issues are recognized and fully addressed, often within minutes and with a strong commitment to respond to all queries within 24 hours.

3.13.2.3 Chia Cultivation Grants

Chia Network has created a Chia Cultivation Grant Program to fund motivated developers to build exciting tools and applications on Chia.

3.13.2.4 Chia Quarterly Hackathons

Chia plans to hold quarterly global hackathons. In addition a third party has recently completed a successful hackathon with the following results:

- 360+ participants
- 50+ countries
- 60 submitted projects
- 10 winners, with the top 3 from India, US and China

3.13.2.5 Chia Developer Outreach

Chia Network employs several individuals that are solely focused on outreach to the community of blockchain developers and existing blockchain projects in order to drive continued adoption of Chia and ChiaLisp. These efforts have been increasingly successful, with several major projects currently converting over from Ethereum to ChiaLisp to benefit from the advanced functionality and low fees. One highly active team is now developing a next-generation NFT platform that leverages some of the unique functionality that ChiaLisp brings, such as the DataLayer, to create NFTs that have the potential to redefine how these instruments are utilized and valued.

4 Climate Warehouse on Chia

The Climate Warehouse is an ideal use for the Chia blockchain. The proposed implementation includes the following components:

4.1 High-Level Architecture

The Climate Warehouse on the Chia blockchain will consist of the following high-level components:

4.1.1 Data Model Implemented on the Chia DataLayer

The data model is the common element of the Climate Warehouse on which all participants must agree. It consists of a set of data tables and conventions on how they should be populated that will be implemented on the Chia DataLayer technology. While all DataLayer tables may not be permissioned to all parties, every DataLayer table will be able to be validated by the full decentralized network.

4.1.1.1 Sovereign Data

Each registry and independent standard will have its own set of data tables and retains exclusive write access to these tables. This is critical to supporting the bottom-up ethos of the Paris Agreement, as it ensures that every registry participates as a peer to every other, publishing data and being held accountable to the same standards as every other.

4.1.1.2 Multiple Tables

The tables for each participant will follow a common data model and data dictionary across all participants. For example, each participant will have a Project table, Units table, Qualification table, etc. The matching tables from each participant will share a common set of columns and the data stored in each column will be formatted similarly.

4.1.1.3 Data From Other Participants

Every Climate Warehouse participant will subscribe to the tables published by every other participant, ensuring that every participant has the same data. Reporting and analytics that cross participant boundaries will have to append the data from the relevant tables across participants to compile a complete Warehouse-wide view of that data. Non-participants may publish data as well but it will clearly be marked and identified as data from a non-participant.

4.1.1.4 No Shared Tables

All tables in the Climate Warehouse will only be writable for one participant. Upon further requirements analysis, there may be some tables storing common data that is only writable by the governance body.

4.1.1.5 Common Configuration File

The governance body will have to host and maintain a configuration file that participants or observers can download to be able to identify the data tables in use by each Climate Warehouse participant.

4.1.2 Chia Node Hosting Climate Warehouse Data

Every participant will have to operate a Chia validator node. These nodes are the conduit for communication with the blockchain. They also host the DataLayer local data stores.

4.1.2.1 Low Hardware Requirements

As described previously, the hardware requirements for these nodes permit a wide range of computer hardware, including, for example, Intel-compatible PCs as much as 13 years old.

4.1.2.2 No Need for Storage for Block Validation

Normally, a Chia validator node uses storage to attempt to participate in adding blocks to the blockchain. The minimum storage to use with the Chia validator node is 108GB, which may be a challenging requirement for some. Also, providing this storage raises the possibility of receiving rewards in the Chia cryptocurrency, which some governments may not be comfortable with. Fortunately, there is no requirement to provide this storage and participate in adding blocks to the chain. Without it, the validator node essentially functions purely as a tool to monitor the blockchain and submit transactions.

4.1.2.3 Local Hosting

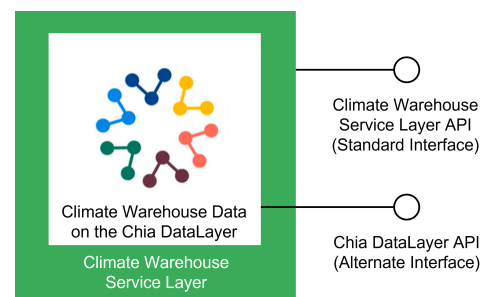
There is no reason to host the Chia validator node at an expensive cloud hosting provider that may be located in a foreign country. Due to the low hardware requirements and the ability to work on even very limited, sporadic Internet connections, even Least Developed Countries (LDCs) should be able to host the Chia node in-country.

4.1.3 Climate Warehouse Service Layer

On the same machine with each participant's Climate Warehouse Chia node will be a Service Layer process for communication with the Chia node.

4.1.3.1 Standard Interface

It is strongly recommended that all applications, including the Auxiliary Application, that use Climate Warehouse data use this Service Layer to communicate with the blockchain. It will provide a standard, Climate Warehouse specific interface for accessing the blockchain to ensure that all participants interact with the data model in a consistent manner.



4.1.3.2 Alternate Interface

More advanced applications using the Climate Warehouse data can access the underlying Chia DataLayer API for more granular access to the data store.

4.1.3.3 Configuration File Parsing

This is the process that will accept the configuration file provided by the governance body, validate it, and then use it to configure the Chia node.

4.1.3.4 Service Layer API

This process will provide Climate Warehouse specific RPC (Remote Procedure Call) interfaces:

- Read data from each DataLayer table and present it in properly named and typed columns.
- Provide notifications of updates detected on chain, and a means to get the rows changed by each update.
- Provide a means of submitting rows to be inserted on the blockchain in properly named and typed columns, and provide a means of submitting rows to be deleted by hash.
 - Provide basic validation of row data to be inserted.
- Provide a means of monitoring submitted transactions until they are fully confirmed by the blockchain
- Provide a means of creating two-party commit transaction files and submitting them to the blockchain.

4.1.3.4.1 Accessible from Any Modern Programming Language

The Climate Warehouse specific APIs will use industry-standard protocols to be accessible using a wide variety of tools and programming languages.

4.1.3.5 Logging

For diagnostic purposes, the Service Layer will provide local logging.

4.1.3.6 Open Source

The Service Layer will be published and licensed as open source software.

4.2 Governance

The Climate Warehouse built on Chia will enable equitable governance.

4.2.1 Sovereign Ownership of Data

Climate Warehouse members will have exclusive access to manage their data. Unless the member delegates that authority to another party, no one else can change the data.

4.2.2 Who Can Participate

There will be many data tables secured on the Chia blockchain. The governance body will aggregate and publish the list of the specific data tables in the Chia DataLayer that are in active use by members in the Climate Warehouse in the configuration file for the Service Layer.

4.2.3 Support for Subnationals and Metaregistries

Countries can delegate read/write permissions to their data tables in the Climate Warehouse to enable subnationals to manage projects in their territories directly, or to enable meta-registries to maintain their Climate Warehouse on their behalf.

4.2.4 Data Model Governance

The governance body will define the data model—the collection of required tables, columns and data types and data semantics—that all participants must follow.

4.2.5 Data Model Change Process

When the governance body finds it necessary, changes to the data model can be published to all participants in the form of a script. Each member can review the script before applying it to their data. As described below, a voting process can be implemented to get consensus on data model changes. Once agreed, all members will need to accept the changes to continue to support the goals of the Climate Warehouse.

4.2.6 Change Testing and Validation

The Chia public blockchain supports a “testnet” that allows testing of data model changes and other changes prior to deployment on the main blockchain. If the testnet is restricted to operate within a VPN, where outside nodes cannot connect and replicate the blockchain and data, then it can be fully deleted when testing is complete.

4.2.7 Double Counting Detection

With all data from all registries in a single repository, straightforward visualizations, analytics and algorithms can be implemented to detect double-counted or fraudulent credits. The Climate Warehouse on Chia is capable of including geospatial data in the form of GIS shapefiles that can be monitored to

identify potential overlap that could indicate double counting. To protect parties, the geospatial data may be permissioned data.

4.2.8 Cancellation Enforcement

The Chia public blockchain is programmable and can enforce process rules to prevent double spending such as preventing retired credits from being restored or transferred.

4.2.9 Support for Coordinated Software Upgrades

The Chia blockchain node software has a regular update cycle to offer new functionality. In nearly all anticipated cases, that software will be backward- and forward-compatible, ensuring maximum compatibility. The governance body can publish updates to the Climate Warehouse API and auxiliary application in tandem with data model updates and each member can accept those updates at will.

4.2.10 Future Capability: Funding Models

The Chia public blockchain also supports secure transfer of digital assets. Observers and service providers can verifiably demonstrate support for the Climate Warehouse by submitting payments or donations to the governance body and announcing the Digital Identifiers they used to do so. Additionally, members can include additional, more detailed data in access-restricted tables and monetize access to that data.

4.2.11 Future Capability: Voting

The Chia public blockchain can support a voting process on proposed changes. Documentation about the proposed changes can be stored and made available in the Chia DataLayer to ensure all parties equally understand the proposals prior to voting.

4.2.12 Future Capability: Dispute Resolution

If the governance body chooses to implement it, a transparent dispute resolution process can be created using the Chia DataLayer. Disputes can be recorded and comments attached. Members can then sign to demonstrate support or dissent. When the issue is resolved, it can be closed by a quorum of members.

4.2.13 Future Capability: Data Aggregation and Presentation

The governance body could run a website that aggregates the public data from all countries and makes it available in an easy-to-use form. This website would get the data from a node that the governance body would run that would not have write permissions on any data.

5 Auxiliary Application

The Auxiliary Application will provide a basic interface for accessing and updating the data in the Climate Warehouse. There is no requirement for Climate Warehouse participants to use the Auxiliary Application. It is provided as an enabler for participants that may not be able to create their own tools to interact with the Climate Warehouse that would be tailored to their existing workflows.

5.1 Portable, Electron-Based Application

To minimize dependencies and infrastructure requirements, the Auxiliary Application will use the open-source Electron framework to be fully portable across PC and Mac and all current versions of the Windows and MacOS operating systems. The Electron framework is essentially a shell that hosts a web browser, web application and backend all in a neatly packaged, installable application.

5.2 Familiar Interface

Because Electron uses HTML to present its user interface, the screens it presents will be immediately familiar and comfortable to most users.

5.3 No Servers

To minimize the technical proficiency needed to install and operate the Auxiliary Application, it will directly access the Service Layer. It will not be a web application that requires a web server, nor will it require a database server. In the simplest case, the Auxiliary Application will be installed on the same computer as the Chia node and Service Layer and will “just work”. It will be able to be installed on a separate computer if needed.

5.4 Manual Entry and Spreadsheet Upload

The Auxiliary Application will support data entry through manual entry and through uploading spreadsheets that follow a prescribed format. The Service Layer will provide interfaces for RPC data insert.

5.5 Export

The Auxiliary Application will support export of subsets of the data to spreadsheet format.

5.6 Support for 2-Party Commit Transfers

When two registries agree to transfer carbon credits from one to the other, the Auxiliary application will facilitate the creation and submission of transfer files and managing the related pending data.

5.7 Installer and Uninstaller

To ease deployment, the Auxiliary Application will provide a standard installer and uninstaller.

5.8 Open Source

The Auxiliary Application will be published and licensed as open source software.