CHIA NETWORK INC.

Business Whitepaper

Version 1.0.1 - February 9, 2021 - revised March 1, 2021

Introduction

Bitcoin and its underlying blockchain are viewed by many as the leading edge of an irreversible, transformative evolution of money, finance, commerce, and society itself.

Bitcoin is whimsically described as “magic internet money.” Those who view that as dismissive are underestimating the transformative impact that programmable digital money is going to have. This whitepaper will attempt to explain the impact that we believe digital money and blockchains can ultimately have on commerce and society. We believe that blockchains applied to money and money adjacent use cases have the power to transform finance, wealth, safety, digital security, and ultimately the entire concept of trust.

As a starting principle, well-designed digital money should be easier to use than cash and harder to steal. Properly formulated, the security of your digital money should not depend upon a team of experts to be secure. Losing keys should be easy to recover from. Anyone, including individuals on their home computers, should be able to participate in the validation of transactions. Anyone should be able to farm -- our version of mining -- instead of a few large powerful entities.

Using well-architected digital money, anyone should be able to be their own bank because it is faster, less expensive, and ultimately safer. We believe that chia, a new digital currency built on our new blockchain with radically different features and security than other digital currencies, will ultimately deliver on the promises of “magic internet money.”

A Brief History: From Bitcoin . . . to Chia

Like all new technologies, the impacts of digital currencies and blockchains are overestimated in the near term and underestimated over the long term. Bitcoin has, to date, led the way just as ARPANET and early ISPs paved the way to the internet, the Web, and ultimately the “there’s an app for that” world in which we currently live.

The more one studies Bitcoin the more subtle, powerful, and fascinating it is. Nakamoto consensus proved that a globally shared database can be trusted without trusting anyone. However, the Proof of Work method that the Bitcoin protocol uses included an assumption that unused CPU cycles are a vast excess commodity in millions of computers world-wide. This premise did not ultimately prove to be correct but it was prescient to search for a vast excess commodity. Specialized single-use hardware and cheap electricity have, instead, become far better at Proof of Work calculations than general purpose CPUs.

This development has weakened another core Bitcoin principle -- decentralization -- as the specialized “mining” hardware is increasingly owned and operated by just a few large entities in purpose-built large data centers located near inexpensive electricity. Thus there has been centralization of what was intended to be a decentralized consensus network. This centralization lowers trust and raises difficult issues regarding electricity consumption, e-waste, carbon generation, and geopolitics.

Eleven years after Satoshi’s whitepaper was released, the world has learned much from the Bitcoin experiment. Research progress in cryptography has also advanced. At Chia, we have set out to harness this experience and stand on the shoulders of giants like Merkle, Rivest, Hellman, Finney, Wuille, Boneh and others to apply new cryptography, some of which we helped invent and refine, to create the next chapter of the Bitcoin experiment.

We are doubling down on Bitcoin. We are adopting and helping Bitcoin adopt new technologies like bech32m, graftroot, and taproot. Chia transaction rates and block sizes are effectively double based simply on more modern engineering. Our coins use a refined version of Bitcoin’s unspent transaction outputs (UTXO) model. Chia is the first new Nakamoto consensus since Bitcoin and utilizes many of Satoshi’s previously un-articulated insights like the fact that natural log governs key blockchain constants related to work difficulty resets. We bring advanced engineering, experience deploying internet scale applications, and scientific rigor to this project.

We have also brought creativity to bear to tackle other important aspects of driving adoption of digital money globally. We have a unique plan to use the corporate, and later public company form, to give transparency, control, regulatory acceptance, and public buy-in, to this new internet money.

We are going to use our expertise in these technologies and go to market strategies to scale out a global open source software support business following in the footsteps of open source pioneers RedHat and MySQL AB. We believe that large institutions, corporations and other entities will be able to reap the efficiencies and benefits of using a digital currency like chia without fear because we will be there to support them.

We are equally focused on the ethos that “Cypherpunks write code.” We will be investing in and supporting developers of all shapes and sizes as they build on top of our base layer blockchain to create heretofore unknown new applications. We consider this our barbell go-to-market strategy. We think that only the largest entities, the smallest individual developers and

individuals, like you, have the need -- right now -- for programmable internet money. Someday we all might buy coffee in San Francisco with chia, but for now we think banks and governments and De-Fi collectives will use it to build new financial technology, solve cross border payments, and invent a new future that doesn't require trusting so many middle men.

We explicitly aim to disintermediate, SWIFT, DTCC, and services like Western Union. However, it would not surprise us if entities like these actually adopt our technologies to improve their offerings - just as record companies did when they finally adopted iTunes and Spotify.

Chia is an attempt to improve on Proof of Work-based blockchains with a new consensus algorithm we call Proof of Space and Time. Instead of consuming massive amounts of electricity and wasteful single-purpose ASIC hardware to validate transactions, Proof of Space leverages the over-provisioned exabytes of disk space that already exist in the world today.

We have observed that many projects and enterprise initiatives that required programmable internet money turned to Ethereum only to discover the harsh limitations of Solidity, Ethereum's smart contract programming language. Poor design and security have made it virtually impossible for enterprise projects to adopt Ethereum to move money or investments in production or at scale. The next most likely alternatives, such as Ripple and Stellar, also have significant issues that force governments and banks to use "intranet" versions of blockchain software on an experimental basis instead. Intranet blockchains are private, permissioned, and have few benefits over a good old fashioned database. They lose all of the positive network effects of an open, decentralized, and secure blockchain.

We believe that central bank digital currency initiatives, financial institution internal tokenization and external payments, global enterprise vendor management, DeX/DeFi, and even personal cross border payments will work best on the Chia blockchain.

Artificial barriers between cash, stocks, municipal debt, corporate debt, futures, and digital money should fall. Such instruments should all be connected to one global market - partially managed for you by your smartphone - that trades all day, every day. Buying stock should be as easy as pressing a button and using Tesla stock to buy a Tesla vehicle or a cup of coffee should be just as simple. Arcane settlement practices should not stand in the way of your desire to trade any specific stock, bond, or futures contract.

You have the right to privately, safely, and securely hold your wealth and hold it in a manner where you can mathematically predict inflation.

You should have the power to very clearly know who you are trusting when you buy an asset.

We also believe that you should be able to securely buy assets and use markets that don't require you to trust anyone.

Chia is green money for a digital world.

Company Vision

We formed Chia Network Inc. for the purpose of driving adoption of chia and to provide controls, trust and transparency in how we use our resources for that purpose. These controls will be especially robust should you choose to become a shareholder once we register our equity on a public stock exchange.

We have seen the scams and farces that have come before our project in this space and we will instead embrace the regulators. It should not be controversial that investors deserve protection through public disclosure and certainly the public shouldn't be sold investments without that legally required transparency.

Chia Network intends to sell software service and support for its open source blockchain and smart transaction software to governments, financial institutions, corporations, and large buyers and sellers of storage. Chia also expects to foster grass roots development of DeFi, DeX, cross border payments, and new end user wallet innovations to accelerate the development of new applications that have not been invented yet but are only possible with a secure, distributed programmable money. Our tools will allow these developers to create applications and wallets that are far more user friendly than what has come before.

The Company has a new and superior approach to funding, building, and supporting a blockchain via an eventually public, for-profit, open source development company that holds a pre-farm (equivalent to a pre-mine) of chia coins. Chia Network intends to list the equity of the Company on an major stock exchange to strengthen the credibility and regulatory certainty of its open source software support business with governments, financial institutions, and enterprises.

The Company believes that its enterprise value will initially reflect the value of the chia held on its balance sheet. As our enterprise software business grows we believe our software service and support business will add to the enterprise value of the Company as well as help drive adoption of chia in commerce and globally. The Chia Network balance sheet should allow the Company's publicly traded equity to function like an ETF for chia coins. The Company expects its equity valuation in a public market to correlate to the price movements of chia coins on digital money exchanges.

Company Operations

The Company was incorporated in the State of Delaware on August 1, 2017 and founded by Bram Cohen, the inventor of BitTorrent. Since its inception the Company has focused on developing Chia Network's blockchain and beginning to promote its potential use. Chia Network's blockchain will be a global open-source decentralized network that operates a payment settlement system using its native cryptocurrency to be known as chia or XCH. Chia Network's blockchain is intended to be more efficient, secure, and easy to use.

The Company is a Delaware corporation based in South San Francisco, California and currently has 21 full time employees and full time equivalent contractors, and 15 part time advisors. Sixteen employees are focused primarily on research and development activities and five employees/contractors focus on the administration of the Company and implementing its business plan.

Company Milestones

Pre Alpha Stage:

In January 2018 Chia Network published Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space academic paper at BPASE '18 and raised a $3.3 million seed round of financing that closed in March of 2018. That round included investments from Naval, A16Z, True Ventures, Greylock, Galaxy Digital, Metastable, and more. In May 2018 we published Simple Proofs of Sequential Work which won best paper at Eurocrypt 2018.

In August 2018, the Company released its first open-source library, bls-signatures, to the public via GitHub. That library and the Company's more recent source code releases have received over seventy five pull requests from third-party developers and have attracted more than thirty five third party contributing developers. Ethereum 2, Dash, and other projects are contributors to components of the Chia Network Blockchain. They are also adopters of portions of Chia Network's new technologies along with Filecoin, and Algorand.

The Company released an open source Verifiable Delay Function (VDF), a Proof of Time primitive for cryptographic protocols in January 2019. In order to optimize the implementation and attract developers, the Company announced a pair of implementation competitions for our VDF. In the two challenges, contestants competed to create faster implementations of the Company's VDF or submit proof of security breaks. After two rounds of VDF competition, the VDF algorithm was four times faster than the original reference implementation. Chia Network subsequently hired one of the contestants and contracts with one of the winners.

In July 2019, Chia Network released its Proof of Space software, its Green Paper, filed its first provisional patents, and announced a Proof of Space competition to optimize the algorithm.

Alpha Stage:

In December 2019, the Company released an alpha wallet simulator and scripting language documentation for Chialisp and an alpha implementation of Chia Network's testnet blockchain.

Beta Stage:

In April 2019, the Company released the beta of the blockchain that included full wallet functionality, transactions, and smart coins on the testnet blockchain. Thousands of developers and community members have installed Chia Network's blockchain software and have nodes on the testnet network.

In July 2020, the Company completed its industry wide collaboration to create the IETF BLS Signature standard and updated our implementation of that standard. With that we were able to finalize our Proof of Space implementation. Since then, our community has been creating plot files that will work on our mainnet (the production blockchain) network.

During the second half of calendar 2020, our un-incentivized testnet was consistently in the top 15 blockchains by public node count. That was despite a quick pace of multiple hard forks (incompatible changes to the blockchain) between releases during that time. Peak network storage of about 30 petabytes, so far, was reached in early January 2021. We estimate that there will be between 40 and 60 petabytes of storage dedicated to the Chia mainnet at launch, yet caution that this is an estimate that could vary widely with a bias to the higher side.

In November 2020 the Company released its new consensus algorithm based on an idea from the paper Proof-of-Stake Longest Chain Protocols Revisited which was presented at Stanford Blockchain 2020 in February 2020. The researchers behind this paper later independently confirmed the original Chia consensus' security guarantees in Everything is a Race and Nakamoto Always Wins which was published in May of 2020.

The new Chia consensus method increases Chia's security to the same 51% attack threshold as Proof of Work with only one long range attack having a lower (~46%) security threshold. That one lower threshold attack is also harder in our new consensus than in our original consensus. The new consensus has additional end user features where transaction blocks arrive approximately every 45 - 49 seconds, generating much more reliable expected block times. There is also faster accumulation of confirmations that more quickly add certainty that a transaction is final. Farming is enhanced by rewarding 64 chia split between 32 farmers every ten minutes during the first three years. There will be a total of four halvings of farming rewards after each three year period.

The Company plans to release the mainnet for Chia Network's blockchain on or before March 17, 2021. There will be an initial period of six weeks where transactions will be frozen and only farming rewards will be rewarded to farmers. This is to stabilize the chain and give additional time for testing.

Market Overview

The Checkered Legacy Financial System

Global banks and currencies are routinely susceptible to exogenous shocks, governmental mismanagement, and financial crises. The global financial system is balkanized, non-transparent, and relies upon outdated technology. Newer financial technologies are typically designed to work only within the jurisdiction of one country. Alternatively, international fintech solutions are often expensive and require complex coordination. Furthermore, incumbent local banks are slow to change, slow to adopt new technologies, and face arbitrary regulatory and political restrictions.

In response to the rise of cryptocurrencies, SWIFT and others are starting to modernize some international transfers. Ironically it remains often cheaper, faster, more traceable, and more time efficient to hand deliver cash to international destinations. Physical delivery of cash, however, has regulatory and security risks like capital controls on imports, capital reporting, limits on export, and theft.

Bitcoin launched during the turmoil caused by the 2008 global financial crisis. Satoshi Nakamoto included the London Times headline “Chancellor on brink of second bailout for banks” in both the Bitcoin genesis block and the source code. Since the launch of Bitcoin, ongoing financial shocks continue to plague the world. Recent global dislocations include the threat of decimation at Cyprus banks, hyperinflation in Venezuela, tightening of capital controls in China, fear of bank account seizure in Hong Kong, Lebanese banks closing to prevent bank runs, the 2019 hyperinflation in Argentina, and the March 2020 COVID-19 induced stock market crash.

Beyond these external shocks, ongoing changes in the banking environment in the post 9/11 world have compelled countries to seek inefficient workarounds in order to conduct legitimate domestic business and to survive with fewer correspondent banks.

These financial shocks have been significant drivers of Bitcoin’s price and adoption.

Decentralized Banking via Nakamoto Consensus

Satoshi Nakamoto invented a process known as Nakamoto consensus, which allows Bitcoin node operators all over the world to safely function as the “bank” for settling transactions even though none of the node operators can individually control the transactions. They are then rewarded with coins for their contribution to validating the network. This process is often referred to as mining and it ensures that no single entity owns or operates the network.

Because this infrastructure is mostly decentralized, internet-oriented and not built on top of a traditional banking infrastructure, it exists globally on any internet connected device, and is usable by anyone. Bitcoin has recently become a relatively liquid global currency, worth over

$600 billion U.S. dollars, with over $55 billion in trading volume on most days. These very metrics have almost invariably increased since we wrote the previous sentence. This global, liquid, permission-less network has launched a new financial technology industry, building on top of Bitcoin instead of a bank.

After Bitcoin came Ethereum, a similar network in terms of architecture and energy inefficiency, but with the promise of an experimental Solidity smart contracting language that has been used to make applications ranging from fundraising tokens to decentralized exchanges and finance (DeX/DeFi), to a virtual cat breeding game.

These two blockchain platforms have experienced growing pains. Proof of Work in Bitcoin now utilizes approximately 87 terawatt-hours per year as of December 2020, a level of energy consumption comparable to the nation of Finland. This level of energy usage is rightly controversial. Bitcoin's brand has also suffered from major attacks on large exchanges, and adoption concerns from business and government related to its association with money laundering and early use in online drug markets. Further, Bitcoin script is limited, slow to develop, and has generally required significant changes in the Bitcoin protocol that can take years to be deployed. These limitations have hampered building superior custody and controls.

Ethereum shares Bitcoin's reliance on "wasteful" Proof of Work mining and has additional problems. Almost every deployed Solidity smart contract that has attracted large balances has in some way been compromised. The Solidity scripting language makes it easier to write financial software than to secure it. Ethereum has become known for the fundraising mechanic known as an "ICO", where the fundraiser creates new tokens on the Ethereum network to sell for bitcoin and ether - many of which have had poor or no regulatory compliance. More recently decentralized financial applications have hinted at a revolutionary change in financial technology but they, too, have been beset by vulnerabilities due to Solidity's poor security stance and the account/global state model used by Ethereum and Solidity.

The Chia Network

Sustainable Nakamoto Consensus using Proof of Space and Time

Chia Network's blockchain relies upon a new Nakamoto consensus algorithm called Proof of Space and Proof of Time. These new methods do not consume the significant amounts of electricity and single purpose hardware that Proof of Work has come to require. Chia Network's blockchain (and chia) is intended to be a "green," eco-friendly alternative to Proof of Work. Unused space is a widely distributed, asic-resistant, and over provisioned commodity. Electricity prices are largely irrelevant to running storage and will become even less relevant as consumer SSD prices fall below hard drive prices. We anticipate that chia farming will be more decentralized than Proof of Work or Proof of Stake and significantly less energy and resource intensive.

Satoshi Nakamoto chose Proof of Work to solve critical problems around trusting a crowd of anonymous individuals to agree upon a transaction ledger. Online it Is relatively easy to fake multiple personas so that one individual might look like 1000 different people on a social media platform. Proof of Work forces each individual or entity to exert some provable effort that makes it unlikely that they control more than one logical account or supposed persona.

Additionally, Proof of Work creates a way to choose the next person who will validate a block of transactions in a way that is mathematically proven to be random. This gives participants in the network assurance that the person who validates their transaction will not be the same person they just sold a boat to in order to avoid an outcome where the validator could make the payment to the boat seller disappear and thus never show up as a completed transaction. Randomly choosing the validator of the next transaction block prevents the boat purchaser from sailing away without making payment or double spending it. Satoshi had hoped that the "unit of work" would be the unused CPU capacity on everyone's computers. However, the algorithms that have the needed properties on CPUs are susceptible to being accelerated in purpose built ASIC chips that drive the cost of proving work towards the cheapest sources of electricity. That gives those with significant capital and access to cheap power the ability to prove far more work per minute and dollar than someone using their laptop at home.

Proof of Space is a way to prove that you are keeping some storage unused on your hard drive. Users of Chia Network's blockchain will plot unused space on their hard drive, by installing software which generates and stores a collection of cryptographic numbers on disk into plots. These users are called farmers, as opposed to Proof of Work's miners. When a new block is broadcast on the Chia Network's blockchain, farmers will scan their plots to see if they have a number that is close to the new challenge number derived from the previous block. This operation of checking for a Proof of Space is fast and very efficient - farmers are known to farm a petabyte on one Raspberry Pi. A farmer's probability of winning a block is the percentage of the total space that a farmer has compared to the entire network for each challenge and there are 4608 chances to win a challenge per day on average.

Using storage as the commodity to secure the unique identity of the next verifier has the properties that Nakamoto hoped for with idle CPUs. Enterprises and end users tend to buy more storage than they're going to need today in anticipation of their future storage needs. Importantly, there is no technological way to store random data more cheaply per terabyte than by leveraging unused hard drives and SSDs made by Seagate, Intel, Western Digital, Samsung and others. Storage also has the property that when someone is done farming, they can repurpose it to other valuable uses like storing a corporate database or adding more pictures of their kids. These Proofs of Space also give excellent assurance that the winning farmer who will validate the next transaction block will be chosen at random.

Since Proof of Space takes very little time to look up and in order to protect against attackers with a lot of space creating alternate competing transaction histories and futures, the Chia Network blockchain has a second component called Proof of Time. Proof of Time requires actual "wall clock" time to pass between blocks. Proof of Time is implemented by a Verifiable Delay Function that takes a certain amount of time to compute but is very fast to verify. The key idea of a VDF is that it requires sequential computation, so having many parallel machines or CPUs/GPUs/ASICs (as in Proof of Work mining) does not create a benefit, and thus electricity waste is minimized. Not everyone needs to run a VDF server (we call them Timelords), but users who wish to add more redundancy and security to the network can do so as the fastest one will always finish first and it takes only one Timelord on the network to complete a block and move the chain forward. Proof of Time also adds additional assurance that the next block's validator will be chosen in a fully unpredictable way so that a user can have confidence that it is very unlikely that a party interested in their current transaction will be chosen as the next validator.

Like Bitcoin, work difficulty on Chia Network's blockchain is dynamically adjusted so that 32 blocks are completed with a target time of 10 minutes on average. Not every block is a transaction block and there are expected to be 9 to 14 transaction blocks every 10 minutes. Farming difficulty adjusts based on both the amount of network space and the speed of the fastest Timelord to keep the target times regular. Regardless of which one changes, if blocks are being released too fast, difficulty is increased. If blocks are being completed too slowly, difficulty is decreased. As farming competition goes up by adding more space to the network, farmers can expect rewards from a particular amount of storage to go down.

Chialisp

Chialisp is Chia Network's smart coin language based on the functional language Lisp. Almost everything on the chia blockchain is a coin. Smart coins deliver smart contract and smart transaction capabilities in one package. Chilalisp has been designed for security and simplicity, while allowing for powerful and broad functionality. Applications running on Chia Network's blockchain are intended to have functionality appropriate for banking, payments, and financial applications. The primary focus for our launch will be on core functionality such as financial controls, payments clearing and settlement, and managing the issuance of assets.

Chia Network's blockchain will enable users to customize custody and clearing arrangements. Chialisp will allow chia controls to match and exceed internal accounting controls and to safeguard funds from accidental loss, theft, or hacking with various risk tolerance levels in an auditable manner. Chialisp is designed to easily have smart coins serve as controls for an SSAE 18 SOC 1 or SOC 2 report and to be relied upon for a GAAP or IFRS financial audit.

This may sound boring to those who have not self-custodied digital money, but for those who have, it makes carrying around digital money feel less like walking through the bad part of town with cash falling out of grocery bags, and more like having your own portable bank vault.

Chialisp will operate within the simple and reliable approach used in Bitcoin of keeping track of currently spendable coins as the only shared state (the UTXO model). Chialisp features enhanced support for net settlement by allowing transactions which open and remove payment channels to be indistinguishable from normal transfers. Chialisp's rules are enforced on the blockchain for superior security of those controls.

With the launch of Alpha Testnet in December 2019, Chia Network made a set of reference smart coins and wallets available to developers and deployers of chia. The initial use cases that Chialisp reference smart coins cover include advanced multi-signature support, atomic swaps, authorized payee whitelisting, withdrawal clawback escrow, withdrawal rate limiting, slow paper wallets, digital identity wallets, and Coloured coins. The Company published reference smart coins for coloured coins in April 2020 and expects to release a digital identity smart wallet shortly.

Coloured coins are Chia's implementation of so-called "colored coins." This is a term of art that loosely describes a class of methods for representing and managing real world assets on top of a blockchain. Chia Coloured coins will be represented by a smart coin embedded into a few of the smallest denomination of chia (a mojo, which is one-trillionth of a chia) that allows an asset to be defined and issued by anyone on top of Chia Network's blockchain. The issued assets will also inherit all of the Chialisp smart coin functionality so that they can have all the custody and controls that native chia enjoy. Adding DID (Distributed Identity) wallet functionality will allow an issuer to only automatically issue an asset to someone who has completed KYC/AML or been verified by a national registry but in a way that is privacy protective and relies upon the W3C Decentralized Identifiers standard.

Multi-sig and Atomic Swaps:

Multi-signature and atomic swaps are building blocks for more sophisticated smart transactions and core to many simpler controls and custody arrangements. This allows a corporation to require two out of three signers to spend money out of a wallet or to complete a trade between bitcoin and chia in a way that requires trusting no other party to propose and complete a swap. The IETF BLS signing protocol also makes multiple signature schemes easier and much safer for the participants as signatures can be merged and don't have to happen in order or at the same time or place.

Authorized Payee Wallets:

Authorized payee whitelisting allows, for example, a corporation to delegate spending authority from a controller to a payroll administrator where the administrator can only make payments to the chia addresses that the controller or CFO set. This mitigates the possible consequences of a successful email phishing attempt or hack on the payroll administrator. This also makes embezzlement difficult. We intend to use our distributed identity wallets to make this especially flexible but have first implemented our reference version of this in a parent wallet, child wallet format.

Transaction Clawback:

When one organization sends coins on a blockchain to another organization, there are two things that need to occur. A certain amount of block confirmations have to happen to prove to the recipient that the coins sent are valid and not a double spend where the coins received will not be considered valid by the network in the future. The second activity is simply the recognition that a payment transaction is actually in process as it may take some minutes to be considered final by the recipient. Withdrawal clawback escrow adds a time period in which the sender can claw back the funds after the initial transfer moves onto the blockchain. By adding a third key that can claw back or accelerate the transfer of a transaction's underlying coins one can lower the risks of sending a transaction and implement escrow business models. With a short recovery escrow period - as an example 1 block less than the recipient's number of blocks they would otherwise consider final - a sender can now correct a typo in a recipient address by detecting the error after sending the transaction, clawing the bad transaction back, and resending a corrected transaction. For certain heavily controlled use cases, one can implement a longer clawback period which allows all transfers from a wallet to be audited and un-done if they are later found to be improper. In a mail order model the consumer could delegate the recovery escrow period to a shipping company that would release the funds to the retailer when the shipper receives the package or return the funds back to the buyer if the goods aren't sent to the shipper in an agreed time frame.

Rate Limited Wallets:

Withdrawal rate limiting allows the creation of wallets that can only spend a certain amount of coins over a specified amount of time. You can put a year's worth of living expenses in a wallet but restrict it to only allow spending 1/52nd of the funds in the wallet each week. If the wallet were stolen, or compromised by a third party, you can use the primary wallet to pull back the balance of the funds that were not yet stolen once it was recognized that control had been lost. Chia shipped a reference rate limited wallet to testnet in August 2020.

Slow Paper Wallets:

Current cryptocurrency best practices are to keep a paper wallet backup of your active or hot wallet. This is prudent for many reasons including that hardware can fail and it's easy to have your hardware lost or stolen. However, this leaves you vulnerable to someone stealing your paper wallet and having complete control over, and ability to steal, all of your funds. Slow paper wallets allow you to store a smart transaction that's capable of starting a time delayed process to recover your funds in your hot wallet but it is not a duplicate of your private key. If someone were to steal your slow paper wallet and start that process, your active wallet can recognize the situation and instead redirect the funds transfer to a new wallet you control. Starting the backup recovery can optionally require a security deposit to further hinder attempts to steal funds via the slow paper wallet.

DID Wallets:

Chialisp enables digital identity wallets that have in depth recovery options and allow individuals and organizations to add identity and permissioning on top of a permissionless blockchain. Users can pseudonymously delegate control of their identity to family or legal counsel in a way that can be recovered by both the delegates and in a way that allows the delegates own identity to be recovered and used as well. This enables certain types of trust/trustee relationships and is a path to digital inheritance. This also allows the provider of an asset on Chia Network's blockchain a method to have end users complete processes like KYC/AML and present that attestation from their digital identity wallet to be able to receive equity, a subscription to a hedge fund, or a government backed stable coin. The asset issuer or verification service can also easily revoke those credentials if they determine that someone's status has changed.

Coloured coins:

Coloured coins allow individuals, financial institutions, corporations, and governments to issue on-chain assets that inherit the smart transaction capabilities of Chia Network's blockchain and rely upon the globally decentralized secure validation that Proof of Space and Time provides. ERC-20 tokens are currently the most recognized form of colored coins, but they are very limited. The Solidity smart contracts they depend on are plagued with security risks. Additionally, they do not feel like a native part of the Ethereum blockchain to end users and require each asset to be individually enabled by wallets and digital money exchanges. Recent security

research has shown that they are vulnerable to being counterfeited on exchanges too. Chialisp coloured coins inherit all of the capabilities of Chialisp which makes them far more suitable to high compliance asset issuance and allow them to be more native to chia wallets.

Unlike Solidity, Chia coloured coins can be used to create ephemeral value and thus applications on the Chia blockchain don't generally require flash loans. This has been one of the achilles heels of DeFi on Ethereum. Ephemeral coloured coins combined with Chia's native exchange capability and partially completed transactions of arbitrary complexity are superior building blocks for the kind of arbitrage applications and transactions that DeFi projects are attempting to build.

Applications of Chialisp:

On the enterprise side, a US based hedge fund could leverage chia coloured coins to manage subscription ownership and have investors present a digital identity that would prove their citizenship, investor qualifications, and KYC/AML status - all natively to Chia Network's blockchain. A government could issue their domestic currency backed stable coin to anyone who had completed a required KYC digital identity certificate. Coloured coins on Chia Network's blockchain can be used for stored or open loop company gift cards, debt issuance, equity issuance, and any related kind of asset issuance, tracking and management.

Because Chialisp is a generalized development language and environment, all of these example functionalities can be mixed and matched as appropriate for a use case. Developers can create new and currently unimagined capabilities with the toolset that Chialisp provides without needing changes to Chia Network's protocol or environment while Chialisp will deliver security and auditability of those controls and applications. We believe that Chialisp will be the best tool for the emerging De-Fi movement.

Chialisp and the choice of BLS Signatures make the implementation of payment channels simpler and more direct than they currently are for Bitcoin or Ethereum. Development in the payment channel space is moving quickly and thus the Company expects to adopt the best technologies from the layer 2 community as they emerge after the launch of Chia Network's mainnet.

The Strategic Reserve

The Company expects to create 21 million chia at mainnet launch (Chia Network's Strategic Reserve or pre-farm) and place those on our balance sheet. The Company established 21 million as an homage to the work that has come before. It is challenging to predict the resources needed to drive adoption of the Chia blockchain, especially those denominated in chia. Thus we hope we are conservatively erring on the side of having an excess Strategic Reserve of chia owned by the Company and ultimately the shareholders. As discussed below, we believe that the public company structure, in conjunction with sound corporate governance, will provide a prudent framework to manage the Strategic Reserve and allow us to distribute excess chia, if any, in a fair way to shareholders using traditional corporate tools.

Post-launch chia Emission Schedule

Farming rewards will create new chia once Chia Network's blockchain is launched. Our farming rewards schedule was directly patterned after the Bitcoin rewards schedule. We present these rewards in an ideal case but reality is usually far from ideal. Due to the fluctuations of space joining the network and Timelord speeds increasing or decreasing, the actual issuance schedule will vary slightly just as Bitcoin's issuance schedule has historically. We may add a time adjustment factor based on what we have observed in Bitcoin to attempt to have farming rewards end up closer to this ideal than Bitcoin did. The idealized schedule is as follows:

- 64 chia will be created every ten minutes for the first three years after launch.
- 32 chia will be created every ten minutes in years four through six after launch.
- 16 chia will be created every ten minutes in years seven through nine after launch.
- 8 chia will be created every ten minutes in years ten through twelve.
- 4 chia will be created every ten minutes for every year after year twelve.

There is no cap, or limit, on the total number of chia that may be created by farming rewards on Chia Network's blockchain. At the end of the sixth year after launch all farming rewards generated to that date will represent 42% of all chia coins in existence at that time. It will take approximately 21 years from mainnet launch for farming rewards to equal the size of Chia Network's Strategic Reserve as trailing emissions begin to slow down in year 13.

Chia Network's blockchain's emissions schedule is known as trailing emissions which adds significant security benefits over capped supply. Capped supply blockchain rewards will eventually completely come only from transaction fees, which might result in miners being incentivized to overwrite recent history instead of mining new blocks in periods where transaction fees are low, particularly if fees are significant during the day and approach zero every night (generally from Midnight Pacific Time to 4AM Pacific), which is the pattern happening today. Because the emission rate is fixed at four chia every ten minutes after year 12, the inflation rate as a percentage of supply is declining forever. Inflation falls through 0.50% in year 25 after launch. The goal is to strike a balance where reasonable transaction fees will be

high enough to strongly incentivize farmers to include them without being so high relative to the fixed rewards that there's strong incentive to overwrite history. We also believe that a fixed supply isn't necessarily what is most important in understanding inflation but that being able to directly calculate a shared expectation of the total supply at any given time gives much the same financial and peace of mind benefit.

XCH Issuance Schedule:

(EOY 1 is End of Year 1)

		EOY 1	EOY 2	EOY 3
Farming rewards		3,363,840	3,363,840	3,363,840
Cumulative farming rewards		3,363,840	6,727,680	10,091,520
Farming % of all XCH		13.81%	24.26%	32.46%
Running total XCH		24,363,840	27,727,680	31,091,520
Halving:		EOY 4	EOY 5	EOY 6
Farming rewards		1,681,920	1,681,920	1,681,920
Cumulative farming rewards		11,773,440	13,455,360	15,137,280
Farming % of all XCH		35.92%	39.05%	**41.89%**
Running total XCH		32,773,440	34,455,360	36,137,280
Halving:		EOY 7	EOY 8	EOY 9
Farming rewards		840,960	840,960	840,960
Cumulative farming rewards		15,978,240	16,819,200	17,660,160
Farming % of all XCH		43.21%	44.47%	45.68%
Running total XCH		36,978,240	37,819,200	38,660,160
Halving:		EOY 10	EOY 11	EOY 12
Farming rewards		420,480	420,480	420,480
Cumulative farming rewards		18,080,640	18,501,120	18,921,600
Farming % of all XCH		46.26%	46.84%	47.40%
Running total XCH		39,080,640	39,501,120	39,921,600

After a final halving, XCH continues trailing emissions:

Halving:		EOY 13	EOY 14	EOY 15	EOY 16	EOY 17
Farming rewards		210,240	210,240	210,240	210,240	210,240
Cumulative farming rewards		19,131,840	19,342,080	19,552,320	19,762,560	19,972,800
Farming % of all XCH		47.67%	47.95%	48.22%	48.48%	48.75%
Running total XCH		40,131,840	40,342,080	40,552,320	40,762,560	40,972,800
Trailing emissions:		EOY 18	EOY 19	EOY 20	EOY 21	EOY 21
Farming rewards		210,240	210,240	210,240	210,240	210,240
Cumulative farming rewards		20,183,040	20,393,280	20,603,520	20,813,760	**21,024,000**
Farming % of all XCH		49.01%	49.27%	49.52%	49.78%	**50.03%**
Running total XCH		41,183,040	41,393,280	41,603,520	41,813,760	42,024,000
50 Year Total XCH		**47,910,720**				

This issuance schedule is directly influenced by Bitcoin's emissions schedule with adjustments for some of the different math underlying the Chia blockchain such as 4608 reward chances per day on average and a quicker pace of halvings.

The following table compares Bitcoin total coins mined during each four year halving period to chia coins farmed during each three year halving period:

	BTC	XCH
First Halving Period	10,500,000	10,091,520
Second Halving Period	5,250,000	5,045,760
Third Halving Period	2,625,000	2,522,880
Fourth Halving Period	1,312,500	1,261,440
End of Year 11*	18,593,393	18,501,120

* - Comparison of actual year 11 outcomes for both, BTC estimated.

Governance of Chia Network's Strategic Reserve

The Company believes that the best way to "govern" Chia Network's Strategic Reserve and support the development of a superior financial infrastructure is to adopt the well tested 400 year old technology of a joint stock corporation and adopt current corporate governance best practices. At an appropriate time, the Company intends to list the equity of the Company on a national stock exchange. The Company's management and use of Chia Network's Strategic Reserve could be material to the adoption of chia for money and money adjacent use cases. We believe that the corporate form with transparent disclosures align incentives better than other current attempts at supporting or governing public blockchains. Of course, due to the network's decentralized nature, Chia Network's blockchain and chia coins that are not held by the Company will work and trade with or without the existence of the Company. The Company has no direct control of the chia blockchain, once launched, as the rules of the chia blockchain can only be updated by having a majority of running nodes independently upgrade to a new version. It is important to note, as we outline below, that the Company does not intend to ever further farm this blockchain. Additionally, unlike Proof of Stake blockchains, ownership of coins has no influence on the governance of, or validation of, the Chia blockchain.

Chia Network established a subsidiary in Switzerland to manage business in Europe. We anticipate establishing a subsidiary in Singapore to manage business in Asia once the pandemic eases. Chia Network's Strategic Reserve will be divided evenly between the US parent company and the Swiss subsidiary at mainnet launch. The Company may use smart coins to limit the total availability of the pre-farmed chia to a vesting schedule once it is able to put it's more sophisticated custody system in place. Additionally, the Company intends to set up internal controls so that its commitments to investors and coin users will require board approval of our independent directors and not be subject to any single shareholder's ability to control Chia Network's Strategic Reserve. The Company also plans to adopt certain assurances that it will not make changes to, as an example, its commitment to not sell chia coins from Chia Network's Strategic Reserve without 90-days' notice to the public. Further the Company does not intend to invest chia coins or dividend coins to shareholders, or use coins to repurchase equity until after we are a reporting company under the 1933 Act and 1394 Act. We outline these controls in the Corporate Governance and Controls on the Strategic Reserve sections below.

Our public company strategy enhances regulatory clarity as the Company intends to become a reporting public company whose equity trades under the regulatory framework of the SEC. The Company believes this will help differentiate the commodity treatment of chia coins from the publicly listed Chia Network Inc. equity.

Public companies create transparency and instill trust in customers like large corporations and governments. That transparency and regulatory infrastructure allows the Company to implement credible controls on how and when Chia Network's Strategic Reserve is used and will allow Chia Network the ability to give the equity markets and the coin markets notice of any changes in policy before those changes can impact either market.

We also want our users, farmers, and developers to have the ability to own a portion of the Strategic Reserve as a shareholder with the investor protections of the US public equity markets. We think allowing exposure to the Chia Strategic reserve to everyone who can invest in equity is a superior way to align everyone's interests in the long term success of chia and the broad deployment of programmable internet money.

The expected correlation between the price of chia on digital money exchanges and the equity valuation of the Company should allow enterprise customers and third parties to hedge between Company equity and chia coins. This will allow organizations that want to use chia in commerce a method to limit their exposure to chia coin volatility. A corporation that borrows chia to finance its international trade can buy straddles and calls on Chia Network's equity to limit their exposure to price volatility in chia coins. This will also tend to move long term investment in the increasing value of Chia Network's blockchain to the equity markets - which currently have broader deployment and ease of access around the globe. We ultimately plan to change that but want to do everything we can to drive adoption today.

Controls on the Strategic Reserve

Our board of directors has adopted the following restrictions on the Company's use of the pre-farm. These may not be changed without a majority vote of the board, which necessarily includes at least 1 independent director.

We intend to have a five person board composed of three outside directors. Currently our board is made up of three members; Bram Cohen, Gene Hoffman, and Chuck Stoops. Mr. Cohen and Mr. Hoffman are not independent as that concept is defined by stock exchange rules while Mr Stoops qualifies as an independent director. Additionally, Mr Stoops is audit committee chair qualified.

We have an ongoing discussion with an additional independent director candidate and have a search open for the third. Once the two board vacancies are filled, the board expects to increase the approval threshold to require a majority of the outside directors as well.

Should any of these controls be so changed, they will not be implemented without at least 90 days of public notice of that change which shall be posted on the Company's website, in its Keybase channels and/or other similar highly visible methods.

It is important to know that if the Company were to find itself insolvent, the fiduciary duty of the directors shifts to creditors and therefore it may not be able to adhere to these restrictions in that unlikely case. Additionally a court order could compel the Company to bypass these restrictions.

These restrictions are as follows:

1. The Company will not sell chia from the strategic reserve. The Company will also not enter into any future contract that would allow or require the Company to later transfer XCH to a third party beyond existing penalty provisions for existing investors as outlined herein.
2. Some existing investors in SAFE agreements (Simple Agreement for Future Equity) have the right to require redemption of a portion of the Strategic Reserve based on the then market price of XCH if the Company has not attempted to file a registration statement in the two years after mainnet launch or effectively registered the Company's equity within three years from the date of the mainnet launch. Additionally, after a registration statement is effective, if the enterprise valuation of the Company does not exceed 65% of the value of the chia on the Company's balance sheet for 30 days, the investor can redeem the amount of their investment at the then market price of XCH. Should these penalty redemption rights ever be triggered they only allow an investor to recover the market value of their initial investment amount at that time and not any gain. The Company expects to convert these SAFEs to equity or preferred equity which would remove these penalty restrictions or replace them with updated ones. Chia Network does not intend to transfer any chia to an investor before a registration statement or an equivalent for the Company's equity is effective.
3. The Company will not and has not compensated employees, employee equivalent independent contractors, officers, or directors of the Company with chia.
4. The Company will not intentionally farm chia on the mainnet. The Company will have farming capacity to support our various testnets but it is realistic that configuration error could cause unintentional farming to occur. The Company plans to put in place controls and monitoring to prevent or detect any accidental farming by Company owned equipment. The Company, however, does not restrict our employees or contractors from farming with their personally owned hardware on their personal time.

The company intends to use the Strategic Reserve for purpose like but not limited to the following:

1. Lending chia to governments, financial institutions, market makers, and enterprises for use in their Chia related projects like asset issuances, paying international invoices, and providing liquidity on various digital money exchanges. These loans will be made to creditworthy entities, will generally require interest denominated in chia and full repayment in chia. From time to time, for marketing purposes the Company may offer negative interest rates to promote adoption. An example would be allowing a storage provider to offer to pay their foreign suppliers 105% of their invoices in chia instead of fiat currency where Chia would only expect 95% of the loan returned.
2. Using chia to fund shareholder activities like share repurchase or dividends to shareholders after we have publicly registered our equity.

3. Using chia to invest in promising projects that expand the functionality of and reach of chia in the markets for money and financial technology but not until we have publicly registered our equity.
4. We may use chia to add additional farming rewards or otherwise incent farmers or developers to validate or develop the network or software. We have a history of running both software enhancement contests and farming contests and plan to use chia as prizes for these sorts of contests.

Again, we do not plan to use chia to fund shareholder activities like repurchases or dividends, or invest in companies or projects using chia until after a registration statement or its equivalent is effective for Chia Network Inc. equity. We believe that the chia blockchain will be sufficiently decentralized shortly after the start of transactions on mainnet such that it would meet the so called "Hinman Test". US Securities regulations generally focus only on the sale of securities so we do not plan on selling components of the pre farm until we have addressed any information asymmetry by becoming a reporting company and we have comfort from our regulators that they do not deem any future Company sales of chia to be a security. However, should they take the position that certain reporting or registration is necessary, we will be in a much better position to meet those requirements as an already public entity.

We believe that these controls are effective and will become more effective as we add independent board members in the first half of 2021. No single shareholder voting alone can modify these controls. Additionally the increasingly independent nature of our board of directors will ensure that the Strategic Reserve is used to thoughtfully increase adoption of chia globally. Upon listing on a national market, these controls will have the additional benefit of securities regulation for their enforcement and binding nature.

The Strategic Reserve is designed to create a long term, sustainable method to fund the ongoing development and deployment of the Chia Network blockchain. Over the long term, our public company structure will give us tools to orderly transfer value to the shareholders and capital to fund the development and deployment of our technology. Should it become appropriate, we may divest the enterprise software or lending business to the shareholders. Ultimately we have the option to create an ongoing development trust fund and fully distribute the remaining assets of Chia Network Inc. to the shareholders leaving a development fund, lending business, and enterprise software business - with the latter two businesses shareholder owned and the balance of the Strategic Reserve in the shareholder's hands.

However, it's very hard to predict ten years into the future, much less thirty years. We think it is important to consider both the long term sustainability of the Chia blockchain and plan to make sure an ecosystem develops with no reliance on any single party. Should the Chia blockchain be as widely deployed and useful as we hope it will be, it will become the rails that banks and governments use to interact globally. That ultimately means that we have to plan to minimize our exposure to geopolitical risks over time but balance that with retaining the resources to actually get to that level of adoption.

Revenue and Go to Market

The Company expects to achieve revenues and build shareholder value primarily through:

- Providing installation, development, and ongoing service and support for the use of chia, Chialisp, and chia smart coins in commerce and issuances of assets using chia Coloured coins;

- Earning interest on loans of chia to market makers, governments, financial institutions, corporations and developers for their use in day to day operations;

- Appreciation of the chia on the Company's balance sheet, due to demand and use of chia by Chia Network's blockchain participants.

Services and Partnerships

The Company will provide services to corporations, financial institutions, governments, and developers that make use of Chia Network's blockchain, Chialisp, and chia. We take a barbell approach to our market. We believe that governments, banks, and enterprises as well as developers, innovative startups, and distributed open source projects have immediate needs for our technology. These services will include, but are not limited to:

- Service and Support Agreements for Software;

- Integration Services into existing corporate Enterprise Resource Planning software or financial institution infrastructure;

- Custom feature / smart coin development / Coloured coin development;

- Integration services into large storage deployments and co-purchase agreements to support large storage deployment acquisition; and

- Building developer tools, supporting and investing in developers, and supporting developer events and hackathons.

The Company will pursue these opportunities with the goal of building a global software solutions team to facilitate adoption and use of programmable digital money both directly and in partnership with other software vendors and financial service companies. The Company believes that just as it took the emergence of Redhat to make Linux safe for corporations and governments to adopt, building a global service and support business that also partners with independent software vendors and software integrators is crucial to the actual adoption of chia for use by corporations, financial institutions and governments in global commerce.

The Company intends to provide custom development, support and joint marketing for other companies and developers launching functionality that uses Chia's blockchain and Chialisp - especially those targeting end users. These partnerships will drive adoption and demand for chia and could also provide the Company with revenue and strategic opportunities.

Digital Money Exchanges

The Company communicates often with platforms that exchange digital assets including digital money. In September 2019 Coinbase announced that chia was one of the seventeen assets they were currently considering for inclusion after those assets launched. In September 2020 Bitstamp announced that chia was one of the digital assets they were exploring support for. The Company expects to provide technical support to such platforms and potentially engage in joint marketing.

The Storage Ecosystem

Chia farming rewards will increase the value of storage in the storage market. Sellers of storage may be able to sell more storage per order as buyers of the storage will know that they can make money from over-allotments of storage. This lowers the risk that the buyer's estimate of how soon and how much storage they need are too conservative. Storage manufacturers can also generate revenue for themselves by changing their drive burn in and quality assurance(QA) processes to plotting and farming chia. Optionally, manufacturers can set up drives for larger customers to have the QA process plot and farm rewards to the farming rewards pool of their customers - again incrementally increasing the value per order for storage customers.

Large storage purchasers, like cloud providers, install storage in their data centers twenty-four hours a day year-round. Due to cloud storage being a low margin business, any incremental decrease in costs per terabyte bought and installed quickly increases margins. Chia Network expects the largest storage purchasers to purchase more storage per order than they otherwise would have and recoup that cost from chia farming that occurs until a higher value use of the storage arises from one of the storage purchaser's customers requesting storage space.

Medium storage purchasers typically don't have full time IT staff solely focused on storage. Much of this market is outsourced to cloud providers who are large storage purchasers. Those that don't tend to purchase storage in 3 to 5 year estimated need increments. Their IT team can focus over a few weeks on installing a new storage area network (SAN) or network attached storage (NAS) and then do nothing but routine maintenance on that storage until months or years later when they add additional capacity. The option to farm chia on the unused parts of that storage will allow buyers and their IT teams to buy and install more capacity up front, which lowers the risk that they underestimated their storage needs and lowers the amount of time the IT team has to spend focusing on adding storage to a SAN or NAS.

End users have traditionally purchased storage on their devices that leaves about 50% of their storage unused on each device. With the transition from hard disk to SSD, the increased price of SSD has led to smaller over-allocations of storage space. However, the market for end user storage is about to pivot to a majority of SSD and with that will come a majority of R&D spending by storage manufacturers on SSD. This is likely to bring storage costs down as fast as they historically have for spinning drives. Industry analysts currently predict that consumer SSD will become cheaper than the equivalent size of hard drive in 5 to 8 years as we discuss below. This will likely return end consumers to buying twice as much storage as they need. We intend to make it easy, via partnerships with storage and device manufacturers, for end users to allocate their unused storage to Chia Network's blockchain and earn rewards directly, or from pools created by the storage or device manufacturer.

The market for used storage is currently somewhat limited. Enterprises tend to retire data center storage after three years. These drives often have significant remaining useful life but can't be trusted for critical data storage as they reach their age of mean time to failure. These data center cast offs are excellent for farming and we believe we will create a market for them that keeps them out of landfills for significantly longer and greener lives.

Two trends in NAND/SSD storage are also promising for chia farming. Certainly by 2031 and probably much sooner than that, consumer SSD will be cheaper than the same size hard drive. This will lead to a significant decrease in the amount of energy needed to farm chia plots. Additionally there is a class of NAND storage that is generally considered waste today that could easily be turned into commercially viable farming space.

Finally, should it turn out that we have underestimated the availability of excess storage and the adoption of chia starts to put pressure on the storage business, the impact will be to drive down the per TB cost of storage for everyone. We consider that a social good even while we hope that the impact of Chia will only be to better utilize existing under-utilized storage space.

DeFi

We believe that Coloured coins and Chialisp are a superior development environment for De-Fi. Inherent properties of Chialisp and our refined UTXO model nearly eliminate the need for flash loans external to a smart transaction to accomplish the same sorts of transactions, exchange, and arbitrage opportunities. Chia's native exchange functionality, via partially completed transactions, will also be an excellent building block for trustless issuance, exchange and price discovery with limited to no counterparty risks depending on the application. We believe that well designed exchange offers and markets will be a superior way to approach things like price discovery as the price oracle problem remains challenging for blockchains and smart contracts today.

Making these sorts of tools available to the unbanked and underbanked, especially in non G-30 countries where the economic infrastructure is far less stable, is very important. Having

alternatives for loans, prediction markets, and futures contracts can have a direct impact on crop yields or small business capital formation that is especially important to the least well off.

International Payments

The Company believes that one of the primary use cases for chia is in international payments - especially in regions whose governments or financial systems are volatile. In the near term, Chia Network intends to support and potentially invest in companies and developers that enable the exchange of chia into local currencies like Localbitcoins and Paxful currently do for Bitcoin. Over the longer term and starting with the storage ecosystem and cloud computing/storage providers, Chia Network plans to enable and drive adoption of chia for settling international invoices in Asia where storage manufacturers and cloud providers source hardware and components. Chia Network's plan to have publicly traded equity will allow novel ways for enterprises to use equity options to reduce their exposure to any underlying coin price volatility while they hold coins for day-to-day use. Chia Network expects significant revenue to be derived from service and support contracts with exchanges and international business and with the associated chia lending interest revenue.

We are equally committed to helping developer partners use our technology and tools to create superior digital wallets for applications like cross border payments. We plan to foster both marketplaces for fiat to crypto like Paxful and the general use case of being able to use your phone to send money home to your family in the country you immigrated from. Options for these services like Western Union are not instantaneous or something you can do from the comfort of home. That is before high fees are factored in. We believe that the economically disadvantaged acutely suffer these higher fees when they could instead have a low fee, easier to use application that saves them both time and money.

Competitive Analysis

The Company believes Chia Network's blockchain and smart coin platform will offer advantages to existing competing platforms. Chia Network's blockchain is subject to competition from both existing platforms, such as Ethereum, "intranet" blockchains like R3, and the traditional financial infrastructure. Financial institutions have largely passed on using Bitcoin and Ethereum beyond the increasingly clear investment use case for Bitcoin. The Chia Network blockchain is more open and accessible than existing financial institutions, more efficient and less wasteful than Proof of Work blockchains, and better designed for secure smart financial transactions than Ethereum while being more decentralized than Proof of Work and Proof of Stake chains.

The Company believes that private or permissioned blockchains are unlikely to gain mass adoption and are analogous to the attempts by corporations in the late 1990's to delay adopting the internet by launching intranets. One of the core values of non-permissioned and public blockchains is that they allow parties that do not trust each other to transact together and alongside each other.

Permissioned blockchains are almost an oxymoron. Blockchains are designed to be universally available and fault tolerant - twenty-four hours a day and three hundred and sixty-five days a year. Adding a permissioning system adds a single point of failure making a permissioned blockchain unable to make the strong assertions of high availability that a normal blockchain has as a basic property. Blockchains follow Metcalfe's law and become more valuable and effective with every additional participant or node on the network. Definitionally, permissioning systems limit the ease of adding new users and thus limits the effect of and value increase of such networks. Governments or enterprises do not obtain the same increases in efficiency from permissioned blockchains as they do from permissionless blockchains.

Permissioned blockchains also severely detract from the trustless trust that a non-permissioned decentralized blockchain creates. It would be hard to imagine the Ukraine joining a Russian permissioned blockchain or Pakistan asking India to allow it to participate in a blockchain that India controlled. Jeff Bezos' Blue Origin would be unlikely to join a space industry trading blockchain run by Elon Musk's SpaceX. But a permissionless decentralized blockchain allows all of these bitter rivals to trust a transaction – even between each other - or on the network right beside their own transactions.

A considerable amount of effort is being expended attempting to solve what we believe are intractable problems with Proof of Stake as an alternate strategy to use less electricity securing public blockchains. To the extent that some projects have created solutions to these problems, we think the tradeoffs that they have made in their assumptions are inferior as they tend to cause centralization and are not as robust as Nakamoto consensus under international geopolitical pressure. Our support of the development and commercialization of VDFs are a source of potential solutions to some Proof of Stake problems as evidenced by projects like Ethereum 2's adoption of an RSA based VDF. VDFs create a source of randomness to mitigate attacks where a validator can influence their own election to validate.

Proof of Stake has three attributes which we think make it a poor choice for a global programmable money. Stakeholders tend to centralize validation towards the richest validators and generally centralize control over time. We think this factor will perform especially poorly when governments become the stakers. Proof of Stake is also susceptible to long range attacks. One can borrow a very large amount of value and stake it for a short period, then unstake and sell the position to repay the loan. Using the chain that still includes the large stake, one can generate an alternative future and introduce it as the new, “better,” chain where the large amount of value was never sold. Finally once someone successfully achieves a 51% attack on a Proof of Stake chain, they have complete control of that blockchain in perpetuity unlike Nakamoto consensus chains that can recover from 51% attacks.

Chia Network’s permissionless and decentralized blockchain will enhance governments and financial institution infrastructure. Banks and payment networks will be able to create funds transfer mechanisms that are secure, fast, and not reliant on any third party – including Chia Network. Governments and banks can safely do business with correspondent banks and vendors around the globe regardless of the geopolitical situation or other nations or banks’ attempts to restrict their activities. An open global decentralized network will make the transfer of money and wealth trustworthy, reliable, and far more efficient without having to rely on middlemen, other banks, or other nations. Chialisp will let them place the restrictions and controls they need on their own transactions or Coloured coin issued assets while letting the underlying value be secured by, and transferable over, a decentralized global network of programmable money.

Executive Officers and Directors

Bram Cohen – Director, Chairman, Chief Executive Officer and Founder, August 2017 to Present

Mr. Cohen is the inventor of BitTorrent, which is the most used protocol for peer-to-peer file sharing over the internet. In 2009, BitTorrent accounted for 43% to 70% of all internet traffic and has recently seen a resurgence in use accounting for nearly 21% of global upstream internet bandwidth in 2018 . Mr. Cohen is often accused of being Satoshi Nakamoto – a claim he denies. Bram founded and was initial CEO of BitTorrent, Inc in 2004. During his time at BitTorrent he worked in various roles as an Engineering Manager, Product Manager, and member of the board of directors at BitTorrent. While there he managed BitTorrent Labs, a research and development department of BitTorrent where he presided over a successful re-architecture of a new BitTorrent client: uTorrent Web. He left BitTorrent in August 2017 to found Chia Network. He has served as Chairman and CTO of the Chia Network since its founding and, since June 2019, as CEO. He is currently an Advisor at Flibe Energy, an engineering company working to design and develop the liquid-fluoride thorium reactor (LFTR). Bram is one of the top selling puzzle designers in the world .

Gene Hoffman – Director, Chief Operating Officer and President, December 2019 to Present, SVP Business Development, August 2019 to December 2019, Advisor to the Board, August 2017 to August 2019

Mr. Hoffman is a serial entrepreneur and former public company CEO. He has built and sold three companies to PGP, Inc., Vivendi-Universal, and Amdocs. From 2003 to 2016 he was co-founder, Chairman and CEO of Vindicia, a consumer subscription infrastructure company sold to Amdocs in 2016. From 2017 to 2019 he was an advisor to the board of Chia Network until he joined the Company full time in August of 2019. He has been a board member at eight different technology and energy companies and serves on two non-profit boards, one of which he co-founded. He has 21 years of working in high compliance security environments with 12 years of managing PCI and SSAE-16 compliance for the storage of 220,000,000 credit cards. Hoffman has built and scaled companies in enterprise software and SaaS, consumer subscriptions, cryptography, and software development. He has raised over $155,000,000 in public and private markets, acquired four companies and sold three. In 1997, he helped end US export controls on cryptography while at PGP, Inc. by personally exporting the PGP Source Code book. Hoffman is co-inventor on several patents and is currently an Advisor at Directly, and Iris.tv.

Mitch Edwards – Chief Financial Officer and General Counsel, January 2019 to Present

Mr. Edwards leads our financial and legal departments. Mr. Edwards has extensive experience as a C-level executive of public and private Internet, tech and blockchain companies. From 2015 until 2017 he was at Overstock.com (Nasdaq: OSTK) where he served as Acting Chief Executive Officer and General Counsel. He oversaw Overstock.com's blockchain M&A

activities, the world's first registered public offering of blockchain securities, as well as development of the t-Zero Exchange, a blockchain securities exchange. Prior to Overstock.com, from 2012 until 2014, Mr. Edwards was Chief Financial Officer & General Counsel for Razer Inc. (HKG:1337), a leading global PC Gaming company headquartered in Singapore, where he led international expansion, M&A and preparation for the IPO. From 2010 until 2012, Mr. Edwards served as CFO & General Counsel of Skullcandy Inc. and was responsible for its IPO, Nasdaq listing and global expansion, and prior to Skullcandy served as CFO & GC for BitTorrent, Inc. Mr. Edwards holds a J.D. from Stanford Law School and received a B.A./M.A. in Jurisprudence and International Business Law from Oxford University, where he was a Marshall Scholar. Mr. Edwards also holds a B.A. in economics from BYU, where he was Valedictorian. He has also worked at the White House, and in the United States Supreme Court.

Chuck Stoops - Director

Mr. Stoops is a 20-year finance and technology industry veteran who specializes in helping high-growth companies transform into global powerhouses. Emerging from a “Big 4” accounting background, Mr. Stoops joined PayPal in 2004 as the second-ranking member of its finance leadership team. While at PayPal, he helped guide the payment company's rapid expansion into international markets, including planning and negotiating its international headquarters investment in Singapore and establishing a fully chartered PayPal Europe Bank in Luxembourg. Leaving PayPal at the end of 2009, Mr. Stoops briefly joined Skype’s Finance team to help prepare the company for a prospective S-1 filing and ultimately a successful sale to Microsoft in early 2011. In 2012, Mr. Stoops became Netflix’s first international hire as its Head of Finance for Europe until the company relocated its European operations from Luxembourg to Amsterdam. By then well-settled in Luxembourg, Mr. Stoops chose to return to PayPal in 2013, this time serving as EU Counsel and Chief Data Protection/Privacy Officer. In late 2014, Mr Stoops joined Japanese multinational Rakuten as its General Legal Counsel and Data Protection Officer for Europe where he, once more, obtained a full European banking charter while managing regulatory affairs and advising the group’s European domiciled holdings; including Viber, Kobo and several national e-commerce marketplaces. Along the way, Mr. Stoops has served as a Board Director for the group companies of eBay, BlackBerry (RIM), Skype and others and is well versed in group financial reporting and controls. At present, Mr. Stoops is a principal in an early-stage banking technology start-up, which plans to receive an EU regulatory license in Luxembourg. Chuck is an active advisor and investor with “exchange space” companies, especially those in the areas of blockchain, payments, identity and loyalty. Mr Stoops is an advocate for any useful financial inclusion project that aids the underserved and underbanked segments of society. Stoops holds a BA from Washington and Jefferson College and two law degrees; a JD from Pepperdine and an LLM from Georgetown Law School. He resides in Luxembourg.

Intellectual Property

The Company licenses its software under the Open Source Apache 2.0 License. The Company currently has provisional patents pending that cover our combined Proofs of Space and Time, our work difficulty resets, our multiple chain methods to stop grinding attacks, and our new consensus algorithm which are all outlined in our Green Paper and our new consensus working document. The Company has trademarked “Chia” and “Chialisp” in major markets around the world and plans to liberally license the trademark for software and applications that are compatible with the Chia Network blockchain. The Company has not licensed and does not rely upon the intellectual property of other companies or individuals for use in the Company’s software or has obtained specific copyright licenses under open source licenses for inclusion of certain dependencies of the Chia blockchain software. The Company may decide to pool it’s patents with others for mutual defensive purposes.

Capitalization

Since inception the Company has raised approximately $16M in funding via SAFE agreements. These have largely been in three rounds with three different standards for price caps, and conversions features. The last round of $5M was completed in August of 2020. No investor has been promised chia in return for their investment. Certain investors have redemption rights that would be denominated in chia at the then price of chia if the Company does not list its equity for public trading over certain time frames as outlined above. The Company expects to convert these SAFEs to equity or preferred equity and does not intend to give investors XCH before a registration statement for the Company’s equity is effective.

Our investors include Slow Ventures, Naval Ravikant, Breyer Capital, Collaborative Fund, IDEO Colab, a16z Crypto, True Ventures, Galaxy Digital, Cygni Capital, Greylock Partners, DCM, Metastable, StillMark Capital, and Kamal Ravikant.

For simplicity, and with the caveat that future valuations may vary widely, we will discuss our pro forma capital structure on an as converted basis assuming a next round of capital raised at a pre-money valuation of $250,000,000.00. The following percentages do not contemplate the dilution a future round at this pre-money valuation would cause. We include in the calculation all issued and outstanding restricted stock awards, options, or warrants to acquire Chia Network stock as if fully vested but not shares reserved for further stock awards that have not yet been issued.

No single shareholder would hold more than 50.0% of the Company. Investors as a group will hold approximately 35.1% of the outstanding shares of the Company on an as converted basis. No single investor or fund will hold more than 10% of the outstanding shares of the Company on an as converted and combined basis. Mr. Cohen will own approximately 47.4% which combines his founder’s equity and his subsequent cash investment in a SAFE on an as converted basis.

Public Market Readiness

The Company has always considered an eventual public offering or listing of its equity to be a component of our product and business strategy. To that end we recruited Mr. Edwards to serve as our CFO and General Counsel and Mr. Hoffman, originally to serve as an independent director but now as President and COO. Mr Stoops was recruited to serve as an independent director who is audit committee chair qualified as Mr. Hoffman no longer meets the independence requirements to serve as audit committee chair.

Since inception our financial statements have been annually independently audited by Armanino LLP who are a PCAOB registered accounting firm. The Company's fiscal year ends March 31 and the Company has completed financial audits from inception through fiscal year 2021. Fiscal 2022 ends March 31, 2021.

Conclusion

The financial future begins now.

Chia is green money for a digital world.

###

- Mulit-sig typo, late ("VDF") removed, "Big 4"
- We inadvertently included our old logo
- SSAE 16 has been updated to SSAE 18
- Smart coins instead of smart transactions