DePINC

The Crypto Currency System Based on CPoST

DePINC Core Team

June 22, 2024

Contents

Chapter 1

DePINC Development

1.1 Crypto Currency

1.1.1 Ripple and B-Money

When it comes to crypto currency, before the well-known Bitcoin, the entire crypto community has begun to experiment on a better international payment channel, such as Dai-Wei's Ripple and B-Money.

Ripple has been used in the settlement between banks in different countries, but never became quite as popular as was Bitcoin, because it is considered too centralized for a crypto currency. Compared to those decentralized crypto currencies, Ripple has always been more appealing to enterprise and business users, but less to the crypto enthusiasts, because its token generation procedure does not involve or incentivize the crypto enthusiasts.

B-Money causes network congestion due to the need for network synchronization in its design. At that time, the network speed was not so fast. During the sending and receiving of currency, network lag often caused problems, sometimes user receives no reply while waiting for a network packet. The system was impractical for mass adoption.

1.1.2 Nakomato Consensus

Then Bitcoin came to stage with its own Nakamoto consensus, which is the asynchronous PoW consensus. In the early days, no one was optimistic about this project. The consensus did not use simultaneous transactions to ensure that transaction results are right, but instead adopted a very interesting mechanism: the longest chain. That is to say, in this distributed system, the nodes manipulates packages and composes the chain, which includes the transaction with the correct result. For this specific package to appear, of course, the nodes in this system have to jointly verify. Only given a timeout package and only when more people participate in the accreditation before timeout, will this package reach consensus.

In this system, there is a situation where nodes can collectively do bad things, so that the correct transaction is not packaged, and the transmission of the network is invalid. Since asynchronous system avoids excessive communication in the network, it is more suitable for multiple-step transactions, While the risk of this mechanism lies with the possibility of the majority of CPU power being controlled by dishonest nodes. A good example is the later appeared 51% double spend attack. The last thing the financial system should do is to roll back or double spend, that is also why Bitcoin was not widely accepted at the beginning.

Over time, a lot of participants joined the system for the financial benefits. Since the difficulty (for manipulating package mentioned above) of the system raised, the cost of harassing the working system has greatly increased for the bad guys. More stable the system, more profitable being honest rather than being dishonest. At this time, people began to realize the fascination of this crypto currency and numerous fans appeared. After years of difficulty increase, the BTC system has gradually stabilized, making it much harder to do double-spend or rollback. It also inspired the original teachings of Bitcoin, and gathered many crypto enthusiasts. It also inspired the original teachings of Bitcoin, and gathered many crypto enthusiasts. At this time, several new types of crypto currencies had been born or made by forks and copies, many got attacked because of their low computational power. The systems with low difficulty are unsafe and can be easily attacked, while highly available systems need tremendous energy consumption.

1.1.3 Bitcoin Features

Bitcoin was never aggressive on using new tech, but chose to adopt relatively mature technologies to build a safe and reliable Peer-to-Peer cash system. The more validated and simple the technology is, the more secure and trustworthy the system will be. For example, the SHA256 algorithm in Nakamoto consensus, is designed by NSA (US National Security Agency), with proven reliability. It seems that the initial design never considered the current ASIC (Application-Specific Integrated Circuit) and power monopoly issues, but focused on pursuing ultimate system security, even sacrificed some of the high efficiency or high concurrency features of internet.

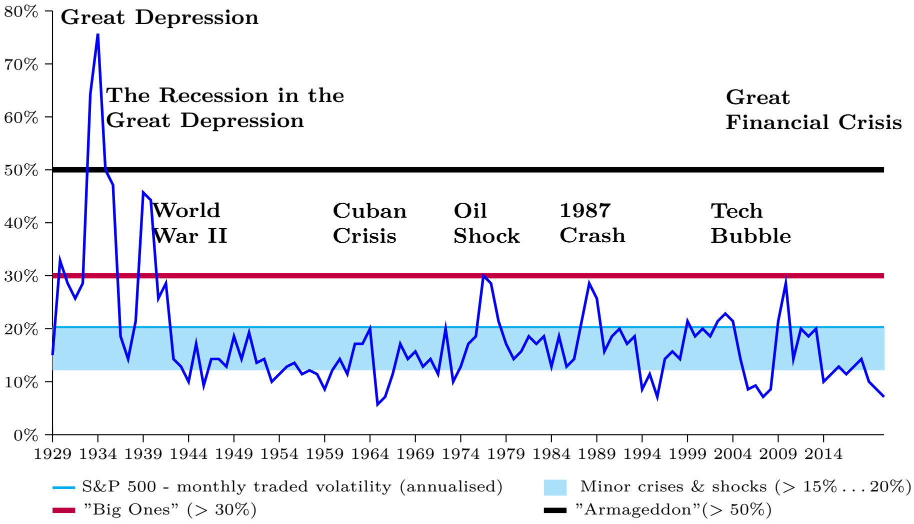
1.2 The Four Major Problems

Monopoly, centralization of computing power, high energy consumption, and the incompleteness of existing PoST have become the four major problems in the Crypto industry. From the beginning of its design, DePINC is aimed at solving the four major problems.

1.2.1 Monopoly

Since its inception, Bitcoin has always had the mission to solve financial institutions' crisis of confidence and issue of monopoly. Since the financial crisis in 2008, Nakamoto believed that the centralization of the financial system would lead to repetition of the history, thus decentralization could be an effective solution for the economy.

The greatest financial crises in the past 90 years



So after all these years, what is the current status of Bitcoin?

The technology of Bitcoin-core is controlled by the core developers, and the code update speed is very slow, which can be described as code-centralization. Bitcoin's computing power is tremendous, ordinary people and personal computers cannot take part and can only trade in exchanges, which indicates hash-power-centralization. Bitcoin's block generation time is relatively slow, about 10 minutes per block, single digit TPS (Transaction per second) cannot provide the same experience as the current internet. Bitcoin core wallet did not make any UI/UX enhancement in ten years, and there is neither a core mobile version, nor any consideration of the current user experience, which indicates user-experience-centralization. Some people are planning to deploy lightning network, allowing more centralized companies to join the nodes, turning the Bitcoin system into a centralized payment system with far worse user experience than visa.

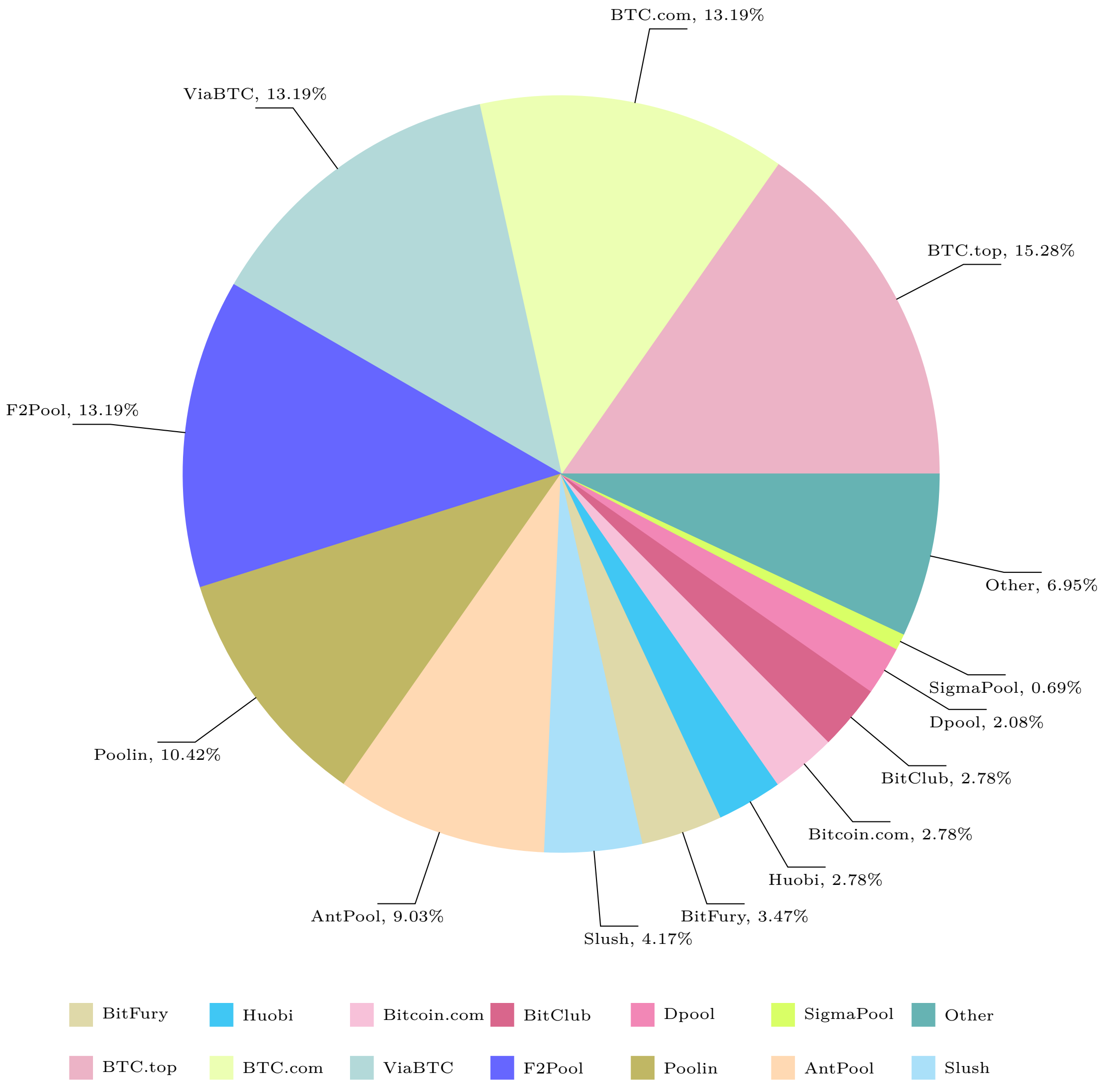
Many believes that the existing Bitcoin system needs to be changed or overturned, keeping the decentralization spirit and involve everyone in this revolution. DePINC has a more economical decentralization approach, using lower cost storage instead of CPU/GPU power. If we believe that centralization can cause crisis to reappear, then we need to know that monopoly has to be eliminated to avoid any risk of potential crisis in the crypto world.

1.2.2 Power Centralization

We mentioned, the main reason for Bitcoin to prevail and be successfully used as the digital money is that its hash power has been maintained at a relatively high level. In 2017, Bitcoin hash power was 4400P, daily production was 1,800 coins, every peta hash power generated 0.4 Bitcoin on average, and consisted of 166 units of 6 tera hash power mining machine. Here comes the issue, the price of Bitcoin can be influenced by mining machine manufacturers through adjusting the price of the mining machine. Thus as crypto currency participants anticipate an increase in Bitcoin's earnings, everyone is willing to mine with higher hash power machines, and enjoy a higher possibility to get rewards through packaging. The top four companies in Bitcoin mining account for about 53% of the mining share; The Ethereum system has a higher concentration ratio, the top three mining agencies account for 61% of the mining share. In addition, 56% of the world's Bitcoin mining software and 28% of Ethereum mining software are concentrated in the data center, showing that Bitcoin's operations are more corporatized.

The figure below shows that now Bitcoin's hash power is about 30,000P - 40,000P. Compared to year 2017, the hash power has increased by 10 times, which means the difficulty has also increased by 10 times for participants.

As shown in the figure below, the hash power has begun to be corporatized, or organized as pools nowadays, e.g. F2Pool, AntPool, Slush.



As hash power gradually increased, the mining machine manufacturers raised the difficulty of coin generation by making devices with improved configuration, kicking out many out-of-date device holders and discouraging a large amount of new entrant.

DePINC solves the problem by using hard disk related consensus to disperse centralized hash power. In the existing PoW crypto currency, each collision of the hash value requires a large amount of calculation, which is of course also a method of managing difficulty. DePINC writes the results of each collision on the hard disk in a pre-computed way. This is also a common time-for-space method to reconstruct the entire calculation. That is to say, under different block difficulties, it takes time and calculation, which takes power consumption differently. While in the DePINC system, as long as the hard disk has enough storage space to contain a sufficient amount of answers the system can involve every crypto enthusiast in the block generation process, without the need for repeated large amount of calculations.

Bitcoin block generation process is roughly like the scrabble game, combining hints with given characters to form a complete word. It is hard for beginners to figure out what the word is, and not easy or at least time consuming even for the veterans. Comparatively, DePINC is more like using a search engine, e.g. Google, to find the word, since the results are all pre-calculated. So the more words in the database, the higher the possibility to get the result. Compared with Bitcoin, DePINC has a much lower barrier to entry, and is much more accessible for every individual.

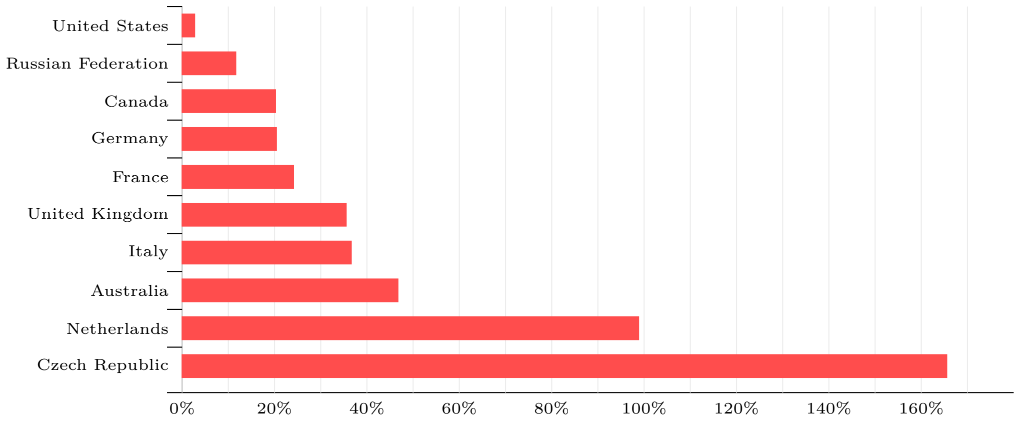
The problem of hash power centralization can be resolved through such a space-for-time approach. Of course, this is just one of the problems DePINC targets.

1.2.3 Energy Consumption

The concentration of hash power also brings about the problem of high energy consumption. So how much resources does the specific calculation consume?

To give an example, the current energy usage level of Bitcoin is enough to generate electricity for 10% of Italy, as shown by the figure below. That is to say, the resources used by Bitcoin could meet the needs of Rome, Milan and Venice, with a combined population of 6 million. Just as a popular saying all roads goes to Rome, if the Bitcoin makes its way to Rome, it will also consume all of Rome's electricity.

Bitcoin Energy Consumption Relative to Serveral Countries



Since most miners are in mainland China (e.g. BitMain the famous manufacturer), I will give a Chinese example. Now that Bitcoin's hash power is around 45EHash/s, then in the case of 1 peta computing power and 0.1 yuan per kWh, it takes about 140000 kWh to do the specific calculation, costing an average of 14,000 yuan. China's high-speed railway consumes more than 9,600 kilowatt-hours per hour. For the 5 hour trip from Shanghai to Beijing, the train needs to use nearly 48,000 kWh. The current energy consumption of a Bitcoin is more than enough for a high-speed rail to run a return trip from Beijing to Shanghai.

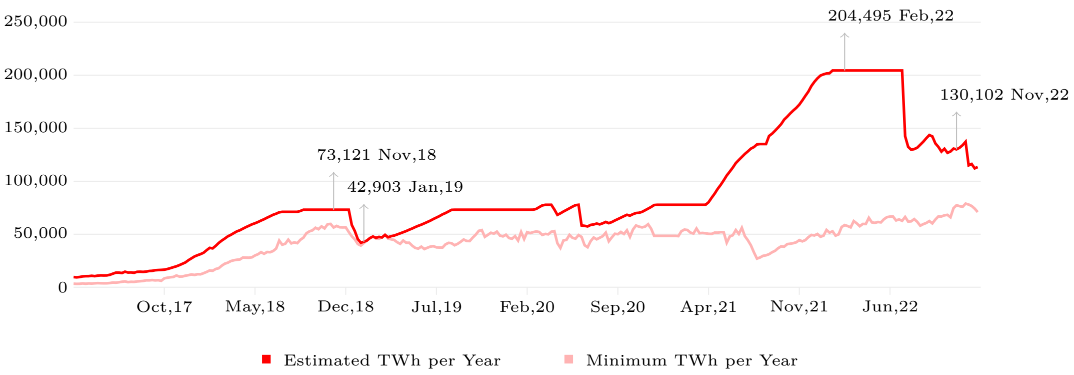
So what is the energy consumption of DePINC?

According to the comparison between a current second-hand S9 and a current second-hand 8 terabyte hard drive, the energy consumption ratio is about 1/300. That is, for 200 USD equivalent of electricity, ASIC takes 1700 watts, GPU takes 250 watts. Comparing those to 8 TB hard disk which cost around 200 USD, the hard disk takes only 5 watts. So for spending on 100 S9 or 100 8 TB hard disk devices with the same total amount of money, the S9 ones consume 122,400 kWh monthly, while for mining DePINC hard disk ones consume 360 kWh, which is equal to only 5 days of electricity for an average American family. That makes DePINC more accessible for anyone interested to participate and contribute in the long term. With such huge difference, the energy saved can be spent on more entities rather than on repeated consumption. Unlike Bitcoin which has slowly become a game for only few, DePINC's low power requirement keeps its door open for many.

Another energy related issue is even more serious: PoW's hash power is reflected in energy consumption, but energy is controlled by the national government in most countries, hence with the expansion of hash power, the impact of energy will gradually increase.

It is shown in the figure below, the energy consumption of Bitcoin was 73,121 TWh in October 2018, and decreased drastically to 44,722 TWh in January 2019. This fall in computing power caused by energy reduction affected the difficulty level of the entire block and the profit of mining machines. This disaster did not only hit Bitcoin. The minor crypto currencies with PoW consensus had to take the risk of forking. It was a deadly threat to the correctness and validity of the entire consensus.

Bitcoin Energy Consumption 2017-2022



That is to say, if the mining pool is concentrated under any centralized institution, then the institution can influence the system's difficulty level and benefits by adjusting the relevant energy resources. The computing power would drop dramatically due to a potential large-scale electricity power decline, which could even cause a PoW coin to fork. The low power consumption of DePINC also provides an effective solution to this problem, through reducing the dependence on energy and taking a block generation approach that is more suitable for long-term survival. The PoS consensus is a low-energy-cost alternative to the current high-energy-cost ASIC based ones. By using the whole global hard disk storage as medium, PoS generates random numbers to guarantee high level of security, and ensures stability of the blockchain infrastructure.

1.3 Seeking Alternatives

1.3.1 Lower Power Consumption

When numerous resources are being used in the mining procedure and costs are gradually increasing, crypto currency enthusiasts have started looking for alternatives to lower power consumption in two different ways: either using new consensus to lower energy cost or using more general apparatus to lower the cost of mass production. The golden age of ASIC mining device and anti-ASIC algorithm implementation had come. The original intention of Ethereum and Monero was to resist ASIC, using a different non-ASIC-friendly consensus to keep the system away from ASIC manufacturers' manipulation while keeping the energy consumption low. However after a period of time, ASIC manufacturers still found ways to design devices that would work with the corresponding algorithm. Among those ASIC ones, Litecoin has to be mentioned. It started with Scrypt which is an anti-ASIC mining algorithm, and soon ASIC manufacturers started producing ASIC mining devices that could work with Scrypt.

As the number of crypto enthusiasts increases, the idea of decentralization has gotten bigger. Of course, everyone who is in the industry wants to be able to benefit. As Bitcoin's energy consumption is increasing each day, mining machine manufacturers are becoming more centralized. The crypto currencies based on PoS is in more demand now than ever. In addition, PoS consensus mechanism guarantees that the difficulty level can be quickly controlled, accumulate enough to maintain the normal operation of the system, and reward the transactions. DePINC is superior to the existing crypto currencies in all the above areas. Its technology has been improved on the basis of Chia, and completely surpasses many other crypto currencies in technical and community dimensions.

Compared to the overhead energy assurance algorithm, we believe that low power consumption can also give the algorithm enough credit to ensure that everyone can use crypto currency in the future in more scenarios.

1.3.2 Proof of Space Time

DePINC provides the perfect solution for the issues mentioned above. It brings a method for crypto zealot to make general apparatus while keeping the energy consumption low. Meanwhile, DePINC maintains a relatively high difficulty level to ensure the stability of the system by using its consensus Proof of Space Time (abbr. PoST). The PoST consensus used by DePINC is also one of the most decentralized consensus mechanisms in this era. Compared with the PoW, where hash power rules, the PoST consensus is ruled by storage power, but slightly different from the cloud storage. PoST utilizes hard disks as a more economical consensus method, so that more people can participate in construction of the system-stabilizing hash power with their own devices. It was the original intention of Nakamoto to design PoW, a decentralized system and an innovative path to real decentralization for everyone, raising consciousness in every new comer to think about and overturn the existing design. DePINC has inherited BTC's spirit, now the new PoST mechanism is responsible for bringing a better future for crypto currency, and engaging more people in the construction of the economic system.

1.4 DePIN Protocol Hub

1.4.1 Integrating algorithms

DePINC aims to establish itself as a DePIN Protocol Hub, integrating validated algorithms for storage and computing. By offering a diverse range of flexible protocol combinations, DePINC provides users with efficient, secure, and flexible decentralized infrastructure solutions all in one place.

Specifically, DePINC begins with reusable storage protocols. As technology advances, DePINC will gradually expand into more protocols covering areas such as computing and data processing. Through this approach, DePINC is dedicated to constructing a multi-layered, multifunctional decentralized ecosystem that comprehensively supports decentralized services for users.

The project's native token is DePC, a novel cryptocurrency based on the CPoST (Conditional Proof of Space Time) consensus mechanism. By involving hard drives as consensus participants, DePINC significantly reduces energy consumption and entry barriers, making the cryptocurrency more secure, decentralized, and accessible to everyone.

1.4.2 Improved Bitcoin

In comparison to Bitcoin, which utilizes the PoW (Proof of Work) consensus mechanism to establish a secure peer-to-peer system, DePINC addresses the issue of high energy consumption and monopolization of electricity resources. Despite the reliability and simplicity of PoW, it disregards concerns over resource consumption and future energy monopolies. With the increasing resource consumption of Bitcoin, more environmentally friendly consensus protocols have emerged. One such protocol is Proof of Space-Time, which, like PoW, ensures security but with significantly lower energy consumption. DePINC adopts this excellent consensus mechanism as a solution to Bitcoin's high energy consumption issues, ensuring network security, system stability, and a notable reduction in energy consumption.

Chapter 2

DePINC's Technical Solution

2.0.1 Algorithms and mechanism

DePINC believes that low power consumption can also provide sufficient trust for algorithms, ensuring widespread use of cryptocurrencies in more future scenarios. By integrating multiple efficient protocols, DePINC continues to drive the development of decentralized technology, offering users a better experience and broader application prospects.

DePINC's Algorithmic Consensus Mechanism The core proof algorithm of DePINC's consensus protocol is PoST, which utilizes Plot files for mining. This approach supports DePINC and enhances network miners' income through composite security with other similar algorithmic projects.

2.0.2 The network parameters

Conditioned Proof of Space Time, or CPoST, would lead the miners, mining pools, the foundation and other participants to engage in a positive business cycle, so that the whole system would always have a dominant temporary commercial vested beneficiary (this vested beneficiary could change with variables such as time, price and mining difficulty) to promote the whole ecosystem.

Total supply	84 million
Development team	2.1 million. Way: pre-mined
Miner	80 million. Way: mining
Avg. block time	3-4 minutes
Initial block size	15 DePINC / Block, 2MB block size
Halve period	In 4 years, the first halving time is about 582688 block height
Current TPS	70 transactions / sec
Stake	Stake amount relate to the computing power
No stake	Only 10% of the block reward.

2.1 DePINC Economic Model

DePINC's economic model / consensus mechanism has been upgraded based on the Chia PoST (Proof of Space Time), and is called: CPoST (Conditioned-Proof of Space Time).

The model will solve the problems listed below:

2.1.1 Economic Model Attack

The main purpose of miners mining is the payback period, and the benefits will inevitably lead to the sale of all mining output, resulting in market crash, lower prices and thinner profits. The CPoST mining model binds miner to its ecosystem, and uses output of mining as future input of mining, to make the entire DePINC system grow automatically.

2.1.2 PoW High Maintenance Cost

It requires a huge amount of power to keep the chain with PoW consensus safe. In good days, it works fine for each part of the system, but in hard times, miners have to pay bills by selling, and it is not easy to keep the miners in the system, if they always have to consider how much energy has been consumed.

2.1.3 Lack of Long-Term Economic Incentive

Without operational incentive funds, the promotional efficiency and market confidence is low. even the core technology might fail to get continuous update. As a result, effective development and iterations are non-existent in the long-run, the team may even create a fork in the subsequent version, and users will no longer be able to tell which is the main-net.

2.1.4 Mining Machine Monopoly

The PoW consensus mechanism will inevitably lead to a race for mining machines. In order to obtain higher hash power, special-purpose mining machines with higher performance will be developed inevitably, and ordinary people cannot participate in mining. The CPoST mechanism is much more accessible because of slow iteration of hard disk manufacturers and low entry barrier. In traditional businesses, the vendor is normally not a competitor to users. But in the PoW systems, the ASIC manufacturer is the biggest miner. It can be easily understood that the miner's competitor is the miner's vendor, since device suppliers take most of the profit by providing mining machines, miner is radically the risk-free arbitrage of ASIC manufacturers.

2.1.5 Power Resources Monopoly

The power resources monopoly leads to no PoW ecosystem expansion, as the cost of mining exceeds the return. For those CPoST miners, the hard disks have much lower power requirement, thus the return of mining is higher. The linear hedge ratio of civil computer hardware can also be taken into consideration to ensure that miners can hedge the price fluctuation risk in the secondary market under the condition of relative safety and cost protection.

2.2 DePINC Architecture and Consensus Mechanism

2.2.1 Bitcoin and Chia

DePINC is derived from Bitcoin and the consensus from Chia's PoST. Bitcoin started in Jan 2009, the stability of wallet and blockchain is widely accepted after 10 years of iterations, it is safe and reliable to implement the

PoS consensus on the Bitcoin QT wallet. DePINC also inherits Bitcoin's excellent P2P network architecture and UTXO system, which is mature and stable. The wallet client could implement any latest developments from the Bitcoin community: lightning network, script upgrades, and much more. The interface standard is kept same as that of Bitcoin, allowing users to integrate easily.

Chia started in August 2017. Combining the advantages of Bitcoin and Chia, DePINC has currently become the most reliable public chain with PoST consensus algorithm. Since its launch on August 3rd 2018, DePINC has grown steadily in computing power, withstood numerous tests, attacks, and cracks, and so far no major loopholes have emerged. By adopting the mature PoST mechanism, a stable and reliable consensus mechanism is introduced to build community confidence in the DePINC public chain. Since being compatible with Chia Plot files, miners can get both DePINC and Chia benefits, with only an additional operation.

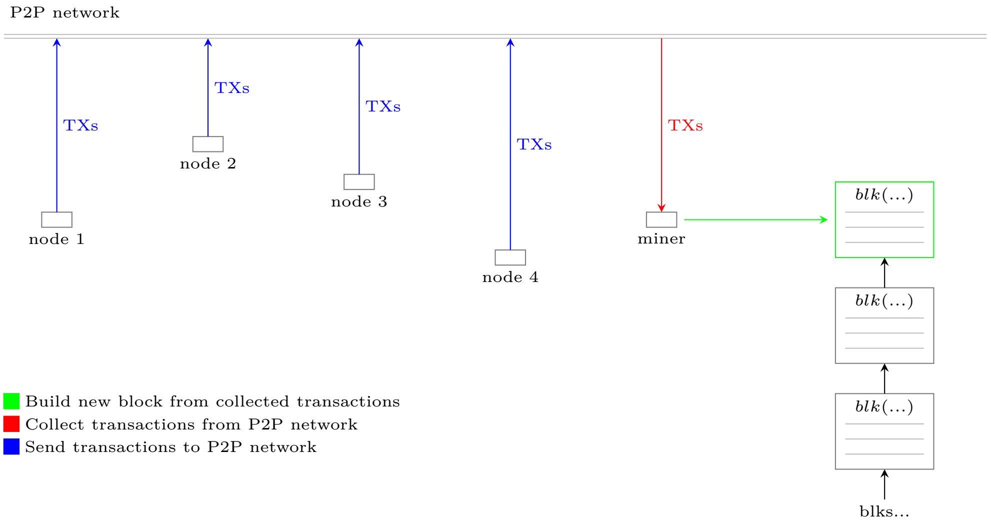
2.2.2 CPoST Model

The CPoST ecosystem model includes mining pool, miner, crypto currency holder, wallet, exchanges and hardware vendor. The positive inner cycle and entrance of outside resources would bring expansion and development to this ecosystem, the rising price of DePINC would attract more miners; more miners coming to the system will lead to further price increase.

The cost of PoW is influenced by four factors: cost of dishonesty, cost of mining, level of difficulty and cost of mining devices. In the end, the PoW would become another low gross margin industry, the former windfall profits was because of insufficient scale, fluctuation of secondary market and limited device vendors. When it comes to PoST, due to the relatively low power consumption by hardware, miners can obtain other coins in the future symbiotic ecosystem of PoST almost free of charge without any risk.

The CPoST system, could give miners the choice to have most of the profits, incur cost for them to be the holder of other PoST coins, and avoid any malicious act. At the same time, the CPoST system attaches great importance to the release of distributional right and packaging right without barrier, which brings equity to the system. DePINC network architecture and the participants:

DePINC network architecture


P2P network
TXs
TXs
TXs
TXs
TXs
node 1
node 2
node 3
node 4
miner
$blk(\ldots)$
$blk(\ldots)$
$blk(\ldots)$
blks...
🟩 Build new block from collected transactions
🟥 Collect transactions from P2P network
🟦 Send transactions to P2P network

2.2.3 Miners Mining Procedure

Plot

Miner plots file at local hard disk, and uses hash value to fill the disk. The larger the storage space, the more hash value could be filled, and higher block generation rate. Hash algorithm uses Shabal256, which is anti-ASIC.

Transaction

Wallet makes up the P2P network(inherited from BTC): Transactions happen between wallets.

Forging

Miner use wallet to listen to the P2P network, once a block is received, the packaging process of the next block starts. Wallet composes a block, sends the hash value of the block to miner, then miner finds the matching nonce. Once wallet receives nonce, it turns the nonce to deadline, wait for the time to end and then broadcast the block.

Verify

Receives the block, verifies it.

2.2.4 Principle and algorithms

Algorithms and acronyms

Decenterialized consensus algorithms require to consume scarce resources, such as computing power, staked money and storage space. DePINC is continuing to use storage space to secure the network. Timelord has been added to provide a reliable cryptographic. By adding timelord to increase the security of entired network.

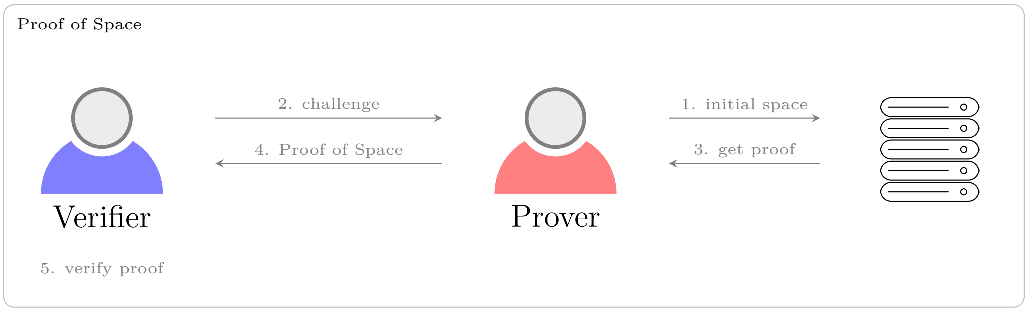
DePINC cryptocurrency system combines Proof of Space (PoS) and Time (PoT). All required proofs are submitted to block-chain and can be easily verified. Miners need to find the correct answer by searching those random-looking data to win the lottery. No funds, special hardware, registration or permission is required to join except a hard driver and internet connection.

Proof of Space

A Proof of Space protocol is one in which:

- A Verifier can send a challenge to a Prover.
- The Prover can demonstrate to the Verifier that the Prover is reserving a specific amount of storage space at that precise time.

The Proof of Space protocol has three components: plotting, proving/farming, and verifying. For more info, see Chia's Details of the chiapos specification, and reference implementation by visiting https://chia.net.



2.2.5 Plotting

Plotting is the process by which a Prover, who we refer to as a miner, initializes a certain amount of space. To become a miner, one must have at least 101.4 GiB available to reserve on their computer (the minimum spec is a Raspberry Pi 4). There is no upper limit to the size of a Chia farm. Several farmers have multi-PiB farms.

As of Chia 1.2.7, a k32 plot can be created in around five minutes with a high-end machine with 400 GiB of RAM, or six hours with a normal commodity machine, or 12 hours with a slow machine using one CPU core and a few GB of RAM. Opportunities still remain for huge speedups. Furthermore, each plot only needs to be created once; a miner can farm with the same plots for many years.

Plot sizes are determined by a k parameter, where $space = 780 * k * 2^{k-10}$, with a minimum k of 32 (101.4 GiB). The Proof of Space construction is based on Beyond Hellman, but it is nested six times (thereby creating seven tables), and it contains other heuristics to make it practical.

Each of the seven tables in a plot is filled with random-looking data that cannot be compressed. Each table has 2^k entries. Each entry in table i contains two pointers to table i-1 (the previous table). Finally, each table-1 entry contains a pair of integers between 0 and 2^k, called ”x-values.” A Proof of Space is a collection of 64 x-values that have a certain mathematical relationship. The actual on-disk structure and the algorithm required to generate it are quite complicated, but this is the general idea.

Once the Prover has initialized 101.4 GiB, they are ready to receive a challenge and create a proof. One attractive property of this scheme is that it is non-interactive: no registration or online connection is required to create a plot using the original plot format. Nothing hits the blockchain until a reward is won, similar to PoW. For pool portable plots, a miner only needs a few mojos to create a plot NFT before plotting and then everything has the same characteristics from there.

2.2.6 Farming

Farming is the process by which a miner receives a sequence of 256-bit challenges to prove that they have legitimately put aside a defined amount of storage. In response to each challenge, the miner checks their plots, generates a proof, and submits any winning proofs to the network for verification.

For each eligible plot (explained later), a miner uses the following procedure to generate a full Proof of Space. Keep in mind that a plot consists of 7 tables (T1-T7) of approximately the same size, as well as 3 checkpoint tables (C1-C3), which are much smaller:

1. The miner receives a challenge from the block-chain
2. For each eligible plot, extract a k-sized value from the challenge, where k denotes the size of the plot (k32, k33, etc)
3. Look in the C2 table for a location at which to start scanning the C1 table
4. Scan the C1 table for the location at which to start scanning the C3 table
5. Read either one or two C3 parks. The number of parks to read depends on the index and value calculated from the C1 table. This requires an average of 5000 reads (the maximum is 10 000). These are sequential reads of 4 bytes (for an average total of 20 KiB)
6. Grab all the f7 entries matching the challenge value (which can be 0 or more), along with the index in the table at which they were found
7. For each matching f7 value, read T7 at the same index where the f7 value was found in its own table, and grab that entry, which is an index into T6
8. The T6 index contains one line point with two back pointers to T5, four to T4, eight to T3, sixteen to T2 and thirty-two to T1. Each back pointer requires 1 read, so a total of 64 disk reads (1 index from T7, 63 back pointers) are performed to fetch the whole tree of 64 x-values.

Since most proofs generated by this process are not good enough to be submitted to the network for verification, we can optimize this process by only checking one branch of the tree. This branch will return two of the 64 x-values. The position of the x-values will always be consecutive and will depend on current challenge (eg x0 and x1... or x34 and x35). We hash these x-values to produce a random 256-bit "quality string." This is combined with the difficulty and the plot size to generate the required_iterations. If the required_iterations is less than every required_iterations those are found from local storage or internet, the proof can be included in the blockchain. At this point, we look up the whole Proof of Space.

By only looking up one branch to determine the quality string, we can rule out most proofs. This optimization requires only around 7-9 disk seeks and reads, or about 70-90 ms on a slow hard drive.

INFO

“Throughout this website, we’ll make a simple assumption that a single disk seek requires 10ms. In reality, this is typically 5-10ms, so we’re using a conservative estimate.

The 10ms estimate also takes into account the time required to transfer data after the seek. While storage industry specs typically assume that large files are being transferred, this does not hold true for DePINC farming, where proof lookups only require a tiny amount of data to be transferred. Therefore, it’s safe to assume the transfer is almost instant.”

DePINC also uses a further optimization to disqualify a certain proportion of plots from eligibility for each challenge. This is referred to as the plot filter. The current requirement is that the hash of the plot ID, challenge starts with 9 zeros. This excludes 511 out of every 512 plots. The filter hurts everyone equally (except for replotting attackers), and is therefore fair.

The plot filter effectively reduces the amount of resources required for farming by 512x – each plot only requires a few disk reads every few minutes. A miner with 1 PiB of storage (10,000 plots) will only have an average of 20 plots that pass the filter for each challenge. Even if these plots all are stored on slow HDDs, and connected to a single Raspberry Pi, the average time required to respond to each challenge will be less than two seconds. This is well within the limits to avoid missing out on any challenges.

Each plot file has its own unique private key called a plot key. The plot ID is generated by hashing the plot public key, the miner public key, and either the pool public key (for OG plots) or the pool contract puzzle hash (for pooled plots). The requirements for signing a Proof of Space depend on the type of plots being used. See the Plot Public Keys page for details on the keys used for plot construction.

In practice, the plot key is a 2/2 BLS aggregate public key between a local key stored in the plot and a key stored by the miner software. For security and efficiency, a miner may run on one server using this key and signature scheme. This server can then be connected to one or more harvester machines that store the actual plots. Farming requires the miner key and the local key, but it does not require the pool key, since the pool's signature can be cached and reused for many blocks.

2.2.7 Verifying

After the miner has successfully created a Proof of Space, the proof can be verified by performing a few hashes and making comparisons between the x-values in the proof. Recall that the proof is a list of 64 x-values, where each x-value is k bits long. For a k32 this is 256 bytes (2048 bits), and is therefore very compact. Verification is very fast, but not quite fast enough to be verified in Solidity on Ethereum (something that would enable trustless transfers between chains), since this verification requires blake3 and chacha8 operations.

2.3 Proof of time (VDFs)

A Verifiable Delay Function, also referred to as a Proof of Time or VDF, is a proof that a sequential function was executed a certain number of times.

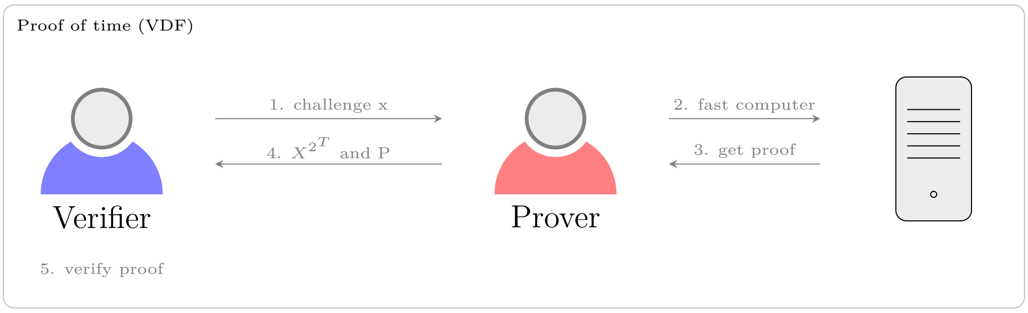
Verifiable: This means that after performing the computation (which takes time), the Prover can create a very small proof in a very short time, and the Verifier can verify this proof without having to redo the whole computation.

Delay: This means that the Prover actually spent a real amount of time (although we don't know exactly how much) to compute the function.

Function: This means it's deterministic: computing a VDF on an input x always yields the same result y.

The key word here is ”sequential”, like hashing a number many times: hash(hash(hash(a))), etc. This means the prover cannot just add more machines to make the function execute faster. Therefore we can assume that computing a VDF requires real (wall-clock) time. The construction that we use is repeated squaring. The Prover must square a challenge x T times. This requires time (T). The Prover also must create a proof that this was performed properly.

Although the following details are not very important for understanding the consensus algorithm, the choice of what VDF to use is relevant, because if an attacker succeeds in obtaining a much faster machine, some attacks become possible.



The VDF used by DePINC is repeated squaring in a class group of unknown order. There are two main ways to generate a large group that has an unknown order:

1. Use an RSA modulus, and use the integers mod N as a group. The order of the group is unknown if you can generate your modulus with many participating parties using an MPC ceremony.
2. An easier approach is to use classgroups with a large prime discriminant, which are groups of unknown order. This does not require any complex or trusted setup, so we chose this option for DePINC.

To create one of these groups, one just needs a large, random, prime number. The drawbacks are that classgroup code is less tested in real life, and optimizations are less well-known than in RSA groups. We use the same initial element for the squaring (a=2, b=1 classgroup element), and instead use the challenge to generate a new random prime number for each VDF, which is used as the discriminant. The discriminant has a size of 1024 bits, which means the proof sizes are around 1024 bits. We use the Wesolowski scheme split into n (1<=n<=64) phases so that creating the proofs is very fast. Since the n-wesolowski proofs can be large, we replace them with 1-wesolowski proofs as soon as they are available. These are smaller, but require more time to make. The proofs themselves are not committed to on-chain, so they are replaceable.

2.3.1 Infusion

As a recap, VDFs take in an input, called a challenge, and produce an output, together with a proof that certifies that the function was evaluated correctly.

A value, in this context, can be thought of as a block with a Proof of Space. The value is combined with an output of a VDF, to generate a new value, which is used as the input/challenge for the next VDF. This is known as an infusion of a value into a VDF.

Therefore, we are chaining VDFs, but committing to a new value in between. This is used so that we have a linear progression of blocks, alternating proofs of space with proofs of time.

2.3.2 Challenge

The DePINC consensus algorithm relies on timelords running VDFs for each block, which are adjusted periodically (and automatically) to take around 3 minutes. During every block, challenges are generated according previous block, and a sort of mini lottery starts, where farmers check their plots for proofs of space. When farmers find a Proof of Space that qualifies, they broadcast it to the network after the VDF calculation with required_iterations is finished.

A challenge is always a 256-bit hash. It is released when a new block has been added to blockchain. The challenge services both PoS and VDF.

2.3.3 Quality and iterations

Quality

The number of quality is used to represent the quality of a proof of space which is found from plots. According the quality, an iterations will be calculated and it controls how many times should be passed before miner can post the block with the PoS.

$$Quality = \frac{QualityString * Plot_{size}}{2^{256}} \tag{2.1}$$

Iterations

"required_iterations" is the number that VDF should run with. To verify a VDF proof not just only verify the proof itself, we also need to ensure the number of iterations is exceeded the requirement from PoS. Smaller of the number means the better quality it is. The block contains with the proof with better quality will be released earlier than others.

$$Iters = Difficulty * Difficulty_{factor} * \frac{QualityString}{2^{256} * Plot_{size}} \tag{2.2}$$

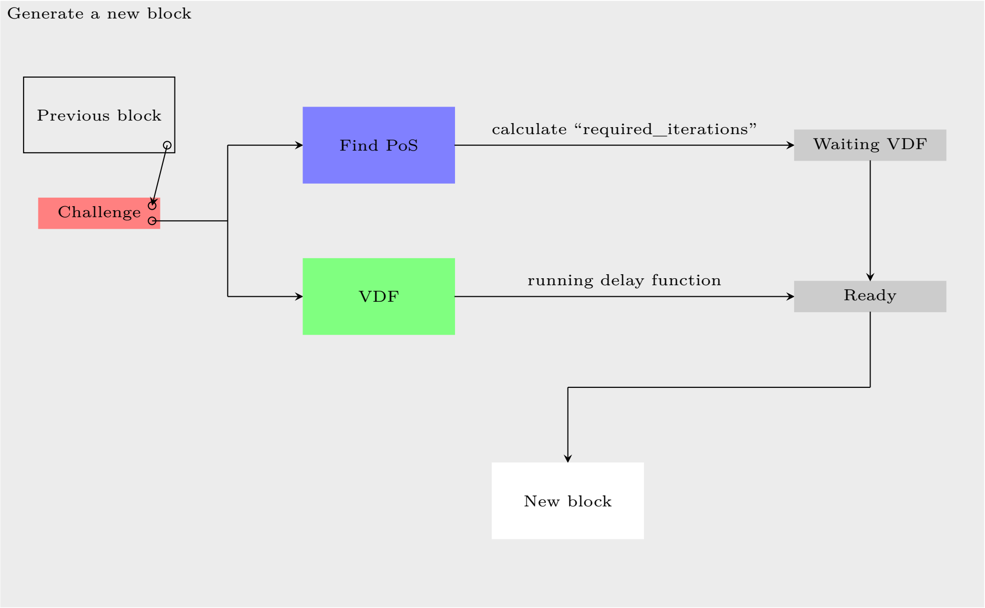
QualityString is mixed from current challenge and proof. $\frac{QualityString}{2^{256}}$ is a number between 0 and 1, multiply the number with the size of plot file will get the quality of the proof. The quality is used to multiply with difficulty in order to get the number of iterations. $Difficulty_{factor}$ is a constant number to fix the iterations to a reasonable range.

2.3.4 Blocks

DePINC releases block every 3 minutes. The basic information are assembled into the block such as transactions, Proof of Space, VDF proofs and difficulty.

Block generation steps

1. Find Proof of Space from plots
2. Calculate "required_iterations" according the proof
3. Wait and retrieve VDF proof from timelord
4. Create new block and pack with all proofs and TXs etc



Void block

There is a very rare situation, the proof of space cannot be found from the entired network. The consensus will add an empty duration without a PoS called void block. After the proof of VDF is calculated, miner will be asked to mix a new challenge to find a Proof of Space. The void block will be included into the new block.

2.3.5 Difficulty

Difficulty is the value represents how good is the block. According to current netspace and VDF speed, difficulty will be adjusted on every block. The time to release a new block will be around 3 minutes.

Difficulty adjustment

The equation of the difficulty adjustment is trying to calculate the new weight of next block. Adjusting difficulty also affects the number of iterations, this is also the way how the new block releases after 3 minutes.

$$NewDifficulty = \frac{Weight_{current} - Weight_{previous}}{Time_{CurrentBlock} * Time_{PreferBlock}} \tag{2.3}$$

2.3.6 Network space

Network space is the value that represents total amount of space those are allocated to generate current blockchain. Network space can be calculated from the difficulty of the last block on the chain.

$$NetSpace = \frac{Difficulty_{current}}{Iters_{current}} * DifficultyConstantFactor * 2^{FilterBits} \tag{2.4}$$

Please note: the calculated size is not exactly the value of the network space. It is just the rule to mesure the network.

2.4 Block validation

2.4.1 Block format

Proof of Space

To verify a PoS, the “PlotId” from plot is required, and we also need the public-key of the farmer (aka “farmer-pk”) to verify the signature later. The plot also needs to be verified to ensure it is owned by the farmer. Record all related fields is the best way to accomplish it.

Name	Data type	Description
Pool pk or Hash	48 or 32 bytes	According Chia's consensus.
Pk type	1-byte	The type of the public key (OG-Plot or PooledPlots)
Local pk	48-byte	Local public-key identify the plot provide the proof
Farmer pk	48-byte	Identify the farmer
K	1-byte	The size of the plot file
Proof	multi-bytes	The proof of space

VDF proofs

Verify VDF proof is more easier. Provide "Proof", "Y", "witness type" and "Iterations" to verify function will get the result. And the verifier also need to ensure the number of iterations is enough to satisify the consensus.

Name	Data type	Description
Y	multi-bytes	large prime discriminant
Proof	multi-bytes	The proof of time
Witness type	1-byte	The type of witness
Iterations	64-bit	The number of iterations

Farmer signature

Farmer signature is used to ensure the owner of the proof of space. The signature can be verified by "farmer-pk". The number of bytes of the signature is 96.

Quality

A 64-bit number represents the quality of proof of space. The way to verify the quality is use the equation we mention before.

Difficulty

Difficulty is a 64-bit constant number represents the network space. The difficulty can be calculated from previous block.

2.4.2 Verify block

The following steps list all required checks to ensure the validity of a block.

1. Check previous block - To ensure the challenge is correct and generated from the previous block
2. Check duration of VDF - The duration between blocks must has a reasonable value
3. Check number of iterations of VDF - The number of iterations must satisify the requirement
4. Check void blocks - Ensure the void blocks are valid and the challenge is mixed correctly
5. Check difficulty - The difficulty can be calculated from the previous block
6. Check the quality of the proof
7. Verify the proof of space
8. Verify the proof of VDF
9. Verify farmer's signature
10. Check distributed amount by coinbase
11. Check validity of pledges TXs

2.5 Economic model

Economic has been improved after the Chia's consensus is updated. The total supply amount is increased and add "lock period" for each pledge.

2.5.1 Total supply is increased

The amount of total supply is increased to 84,000,000.

- The total amount to be supplied in each block will be doubled after consensus updated
- The foundation will receive an additional amount of the total amount multiply with 2 already supplied on the current chain at one time
- The Foundation will no longer receive funds in future blocks.

2.5.2 Pledge improvement

The miner needs to pledge a certain amount of DePINC to the chain, and the pledged amount is related to its pledge time. When the pledge time is less than three years, the pledge amount will be discounted. During the pledge time, these DePINC will not be able to be withdrawn.

Netspace

Assuming that the netspace of a miner is “p”, the current netspace of the entire network is “t”, and the current distributed amount is “m”, then the current miner wants to achieve the condition of full pledge, and the amount of currency “a” needs to pledge is:

$$a = \frac{p}{t} * m \tag{2.5}$$

Lock period

Now the miner needs to select the type of period for every new pledge. It determines the ratio value of the total amount that the pledge amount actual is.

Period	**Ratio**	1_{DePINC} **required**
Current Deposit (1 week)	8%	12.5_{DePINC}
1 year	20%	5_{DePINC}
2 years	50%	2_{DePINC}
3 years	100%	1_{DePINC}

Burn

When the pledge period has not yet expired, it is allowed to lose part of the pledged currency to withdraw the pledged amount, but part of the currency will be destroyed according to the pledged time. Assuming that “p” blocks have been pledged, a total of “f” blocks need to be pledged, and the amount of pledged currency is “a”. Then, withdrawing the pledge with the amount of currency a in block “p” will return the amount “w” back, and $a - w$ is the amount of currency destroyed after this withdrawal.

$$w = \frac{p}{f} * a \tag{2.6}$$

Burning mechanism

DePINC will use a special (20-byte) accountID, it is filled by 0x23 of each byte. No one owns the private-key, and the consensus also prevent that no one will be able to make a new transaction that transfer DePINC from this account even the foundation. All burned DePINC will be sent to this account, and the amount required of mining will be re-calculated on next block.

Total amount update frequency

The number of total distributed amount is calculated once a month (total 20*24*30 heights), and the data will remain unchanged for one month until the next calculation. This means that the amount of currency that all miners need to pledge also changes every month. This mechanism simplifies the calculation of pledges, and miners no longer need to calculate the total distributed amount frequently.

Insufficient pledge amount

When the amount of pledge is not enough for a miner to claim all rewards from a new block, miners will only get 15% of the block rewards, the rest 85% will be locked in the chain until the miner who has enough amount of pledge to claim all rewards.

For example

We assume that there is a miner initialized 15_{PB} storage to do the mining. Assume that the current netspace of the entire network is 200_{PB} and the total supplied amount is $10,000_{DePINC}$. Thus, according to the formula, the total amount that needs to be pledged per PB is $\frac{10{,}000}{200} = 50_{DePINC}$. The miner in order to obtain 100% mining rewards, a total of $50_{DePINC} * 15_{PB} = 750_{DePINC}$ needs to be pledged to the chain.

100% **rewards**

The miner can choose one of the following pledge plans to get 100% rewards:

1. Deposit 9375_{DePINC} to the chain with period "Current Deposit"
2. Deposit 3750_{DePINC} to the chain with period "1 year"
3. Deposit 1500_{DePINC} to the chain with period "2 years"
4. Deposit 750_{DePINC} to the chain with period "3 years"

15% **rewards**

Miner will receive 15% rewards when the amount of pledge is less than 750_{DePINC}. The pledge amount also increases when the total supply is increased or the miner initialized more space to do the mining.

Withdraw an unexpired pledge

The withdrawal amount will be calculated according to the percentage of the pledged period when the pledge is withdrawn unexpired. The remaining amount will be directly burned on the blockchain. For example: there is a pledge with total amount of 300_{DePINC}, the period of this pledge is 3 years. If we want to withdraw it after only 10 months. There are only a total of 83.33_{DePINC} will be withdrawn, the remaining 216.67_{DePINC} Will be burned.

Formula to calculate the amount

$$Withdrawal_{DePINC} = Total_{DePINC} * \frac{Time_{Elapsed}}{Time_{Agreed}} \tag{2.7}$$

2.5.3 Foundation addresses

There is at least one foundation address to be able to use for generating new blocks without binding them with a valid farmer public-key. This is a mechanism to ensure that the network will keep generating new blocks and this allows new miner to create binding/pointing transaction to add miners to the network. Consensus ensures that the pledge amount of foundation addresses will not be able to calculate with full mortgage, even someone deposit pledge to the foundation addresses.

Chapter 3

Tech Roadmap

3.1 Fusion Consensus

1. In 2023, DePINC will be compatible with Chia's old agreement documents for mining.

2. 2025 Fusion Consensus, DEPC is committed to building a flexible, scalable and integrated decentralized protocol ecosystem to meet future challenges and opportunities.

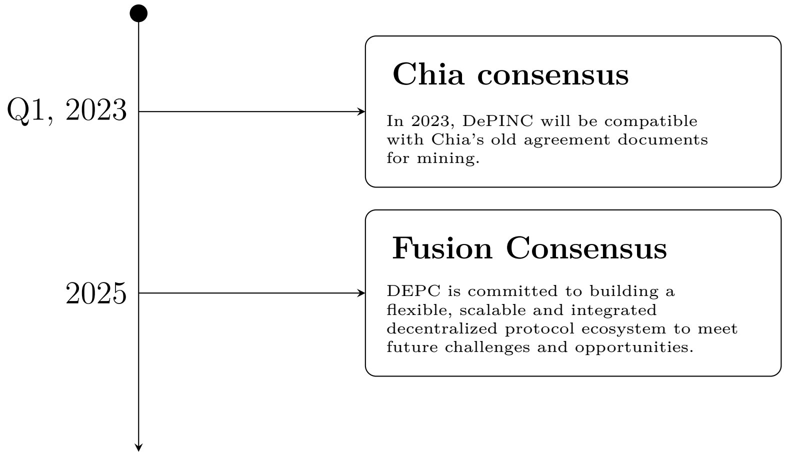
   (a) Dynamically adjust protocols: Flexibly add or reduce protocols based on future development and market demand to ensure the cutting-edge and adaptability of the ecosystem.

   (b) Expansionary economic mechanism: By expanding the scale of the ecosystem, attracting more users and developers, and promoting the widespread application and healthy development of the protocol.

   (c) DePIN Hub protocol with multiple storage and computing functions: Integrates multiple storage and computing protocols to provide efficient, flexible and secure one-stop decentralized infrastructure solutions.

3.2 Outlook

DePINC is committed to becoming a high value financial system that changes the way crypto currencies are produced.



Q1, 2023

Chia consensus

In 2023, DePINC will be compatible with Chia's old agreement documents for mining.

2025

Fusion Consensus

DEPC is committed to building a flexible, scalable and integrated decentralized protocol ecosystem to meet future challenges and opportunities.