ZSToken

White paper

V1.10

Foreword

As the world becomes more and more digital, cryptocurrency is a natural step in the history of currency development. Zs is the first digital currency used in daily life and represents an important step in the adoption of cryptocurrencies worldwide.

As the world becomes more and more digitized, cryptocurrencies have become a natural trend in currency development. The first digital currency used marked a big step forward in the adoption of cryptocurrencies around the world.

Our mission: to build a cryptocurrency smart contract platform that ordinary people can use, which is both secure and easy to operate.

Our vision: Driven by zs (the world's most widely used cryptocurrency), building the world's most inclusive peer-to-peer market. Our vision: Driven by zs (the most widely used cryptocurrency in the world), building the world's most inclusive p2p market.

Currently, our daily financial transactions rely on trusted third parties to maintain transaction records. For example, when you make a bank transaction, the banking system keeps records and keeps the transaction safe and secure. Similarly, when Cindy used PayPal to transfer $ 5 to Steve, PayPal kept deducting $ 5 from Cindy's account and credited Steve's $ 5. Central record. Intermediaries such as banks, PayPal, and other members of the current economic system play an important role in regulating global financial transactions.

1. Unfair value acquisition. These intermediaries have accumulated billions of dollars in wealth creation (paypal has a market value of about 130 billion US dollars), but hardly pass anything on to their customers-ordinary people on the ground, and the money they seize has a considerable share in the global economy A large proportion. More and more people are far behind and out of reach.

2. Cost. Banks and companies pay high fees for convenient transactions. These costs often severely affect low-income people who have no choice.

3. Review system. If a trust agency thinks that you should not transfer your money, it can place restrictions on the flow of your money.

4. License. As an intermediary's credit authority, you can become the gatekeeper of the global network. You can arbitrarily prevent anyone from becoming a member of the network.

5. Privacy. As privacy issues become more urgent, these powerful janitors may accidentally reveal-or force you to reveal-more financial information about yourself than you want.

An anonymous programmer (or group) Satoshi Nakamoto launched Bitcoin's "peer-to-peer electronic cash system" in 2009, a watershed in money freedom. For the first time in history, people can safely exchange value without a third party or trusted intermediary. Paying with Bitcoin means that people like Steve and Cindy can pay each other directly without having to pay agency fees, obstacles and intrusions. Bitcoin is truly a borderless currency that can drive and connect the new global economy.

Bitcoin's "peer-to-peer electronic cash system" was launched in 2009 by an anonymous programmer (or group) Satoshi Nakamoto, and is a watershed in monetary freedom. For the first time in history, people can safely exchange value without the need for a third party or trusted intermediary. Paying with Bitcoin means that people like the statues Steve and Cindy can pay each other directly, bypassing agency charges, obstacles and intrusions. Bitcoin is a truly borderless currency that powers and connects the new global economy.

Introduction to distributed ledgers

Bitcoin has achieved this historic feat by using distributed records. True records, but Bitcoin's records are maintained by a decentralized community of "validators" who are responsible for accessing and updating this public ledger. Think of the Bitcoin protocol as a globally shared "Google Sheet" containing transaction records, verified and maintained by this distributed community.

The breakthrough for Bitcoin (and general blockchain technology) is that although the records are maintained by the community, the technology enables them to always reach a consensus on real transactions, ensuring that scammers do not record false transactions or go beyond the system. This technological advancement allows the removal of centralized intermediaries without compromising transactional financial security.
In addition to the decentralization of distributed ledgers, in general, Bitcoin or cryptocurrencies also have some good attributes that make money smarter and more secure, although different cryptocurrencies are based on different implementations of their protocols May be stronger in some attributes and weaker in others. Cryptocurrency is stored in a crypto wallet with a publicly accessible address and is protected by a very strong private password (called a private key). The private key signs the transaction with a password, making it virtually impossible to create a fraudulent signature. This provides security and indistinguishability. Unlike traditional bank accounts that can be seized by government agencies, anyone without a private key cannot take away the cryptocurrency in the wallet. Due to its decentralized nature, cryptocurrencies are censorship-resistant, as anyone can submit transactions to any computer in the network for recording and verification. Cryptocurrency transactions are immutable because each transaction block represents a cryptographic proof (hash) of all previous blocks that previously existed. Once someone sends you money, they will not be able to get your payment back (i.e. there is no bouncing check in the blockchain). Some cryptocurrencies can even support atomic transactions. The "smart contracts" built on top of these cryptocurrencies not only rely on law to enforce them, but also directly through

publicly auditable code, which makes them untrustworthy and possible to get rid of middlemen such as real estate custody for many businesses.

In addition to decentralization, Bitcoin, or general cryptocurrencies, share some good attributes to make the currency more intelligent and secure, although different cryptocurrencies may be stronger on some attributes and weaker on others, based on their Different implementations of the protocol. Cryptocurrencies are stored in an encrypted wallet identified by a publicly accessible address and are protected by a very strong private password called a private key. This kind of private key is used to sign a transaction with a password. In fact, unlike traditional bank accounts, which can be seized by government authorities, the cryptocurrency in your wallet will never be taken away by anyone with your private key. Due to its decentralized nature, cryptocurrencies are resistant to censorship, because anyone can submit transactions to any computer in the network for recording and verification. Cryptocurrency transactions are immutable because each transaction block represents a cryptographic proof (hash) of all the people that existed before. Once someone sends you money, they can't steal their payment back to you (also, there is no bounce on the block chain. Some cryptocurrencies can even support atomic transactions. "Smart contracts built on top of these cryptocurrencies "Not only relying on law enforcement, but also directly through publicly auditable code, which makes them trust each other, and there may be intermediaries for many businesses, such as real estate custody intermediaries.

Security of distributed ledger (mining)

One of the challenges in maintaining a distributed record of transactions is security-in particular, how to have an open and editable ledger while preventing fraud. To address this challenge, Bitcoin has introduced a new process called mining (using a consensus algorithm "proof of work") to determine who is "trustworthy" for updates, and a new process for sharing transactions

One of the challenges in maintaining a distributed transaction record is security-specifically, how to have an open and editable ledger while preventing fraud. To meet this challenge, Bitcoin adds a novel process called mining (using a consensus algorithm "proof of work"), who may be "trusted", thereby updating the shared record of transactions. You can think of mining as an economic game that "verifiers" prove their value when they try to add transactions to their records. To verify, the validator must solve a complex set of computational challenges. The device "mines" a reward-currently 12.5 bitcoins (about $ 40,000 at the time of writing here).

This process is very secure, but it requires huge computing power and energy consumption, because users are essentially "burning money" to solve the computational problems that allow them to get more bitcoin. The burn-to-reward ratio is so penalizing that the personal interest of the validator is always to post honest transactions to the Bitcoin record.

This process is very secure, but it requires huge computing power and energy consumption, because users are actually "burning money" to solve computing problems and thus earn more bitcoin. The punitive ratio of burning money to rewards is such that publishing honest transactions on Bitcoin records is always in the interest of the validator.

Problem: The concentration of power and money makes the first generation of cryptocurrencies inaccessible.

In the early days of Bitcoin, only a few people were verifying transactions and mining the first block. Anyone who runs Bitcoin mining software on a personal computer can earn 50 Bitcoins. With Bitcoin becoming popular, smart miners can choose, and if they have more than one computer to mine, they can make more.

As the value of Bitcoin continues to increase, the entire company is beginning to rise. These companies have developed specialized chips ("ASICs") and used these ASIC chips to build large server farms to mine Bitcoin. The rise of these well-known large-scale mining companies has driven the bitcoin gold rush, making it difficult for ordinary people to contribute to the network and get a return. Their efforts are also starting to consume more and more computing energy, exacerbating increasingly serious environmental problems worldwide. Through the continuous increase in the value of Bitcoin, a large number of companies have begun to build mines. These companies have developed specialized chips ("ASICs"), and the emergence of these huge mining companies has driven the bitcoin gold rush, making it difficult for ordinary people to contribute to the network and get rewards. And their efforts are beginning to consume more and more computing energy, leading to increasingly serious global environmental problems.

The convenience of bitcoin and the rise of the bitcoin mines have rapidly promoted the construction of the bitcoin network and the concentration of wealth on scale. To provide some background information, 87% of Bitcoin is now owned by 1% of the Bitcoin network, many of which were mined almost free in the early days. Another example is Bitmain, one of Bitcoin's largest mining operations, which has earned billions of dollars in revenue and profits.

The concentration of power in the Bitcoin network is very difficult and expensive for ordinary people. If you want to get Bitcoin,

Your easiest choice is:
1. Dig it yourself. As long as you have specialized hardware (if you are interested, here is a platform on Amazon!) And then go for a change. Just know that since you will be competing with large server farms from around the world, the energy consumed will be equivalent to that of the entire Swiss country, and you will not be able to extract too many resources.

2. Buy Bitcoin on the exchange. Now, at the time of writing, you can buy bitcoins at a price of $ 3,500 each (note: you can buy a partial amount of bitcoins!) Of course, because the price of bitcoin is quite unstable, it will also bear a huge risks of.

Bitcoin is the first technology to show how cryptocurrencies disrupt current financial models, enabling people to conduct transactions without third-party intervention. The growth of freedom, flexibility and privacy continues to drive the inevitable move towards digital currencies as the new norm. Despite its benefits, the (possibly unexpected) concentration of money and power in Bitcoin poses a significant obstacle to mainstream adoption. As the research conducted by the core team at zs attempts to understand why people are reluctant to enter the cryptocurrency space. The risk of investment / mining has always been considered a major barrier to entry.

For the first time, Bitcoin has shown how cryptocurrencies can break through modern financial models, enabling people to transact without third-party obstructions. Freedom, ownership and increased ownership continue to drive digital currencies into a new norm instead. Although Bitcoin has many benefits, its (possibly inadvertent) concentration of funds and power poses a major obstacle to mainstream applications. The core team of zs conducted a study to understand why people are reluctant to enter. People have always considered the risks of investment / mining as a key barrier to market entry.

Solution: zs-Enable mining on the phone

Solution: Implement zs mining on mobile phones

After identifying these major obstacles to adoption, the zs core team set out to find a method that would allow everyday people to mine (or get cryptocurrency rewards by verifying transactions in a distributed transaction record). Recall that one of the main challenges posed by maintaining distributed records of transactions is ensuring that updates to this public record are not fraudulent. Although Bitcoin's process of updating records is proven (burning energy / money to prove trustworthiness), it is not very user-friendly (or planet!). For zs, we introduced additional design requirements using a consensus algorithm that is also very easy to use for users and ideally can be mined on personal computers and mobile phones.

After identifying the key obstacles to these adoptions, the zs core team started looking for a way for ordinary people to mine (or get cryptocurrency rewards by verifying transactions with distributed transaction records). As a guardian, one of the main challenges in maintaining a diverse transaction record is ensuring that updates to this public record are not fraudulent. Although Bitcoin's process of updating records has been proven (burning energy / money to prove credibility), it is not very user-friendly (or planet!) Friendly. Regarding zs, we dated an additional design requirement, which is to adopt a consistent algorithm, which is very user-friendly and ideally can be mined on personal computers and mobile phones.

When comparing existing consensus algorithms (the process of recording transactions to a distributed ledger), the Stellar Consensus Protocol has become the main candidate for user-friendly, mobile-first mining. The Stellar Consensus Protocol (SCP) was designed by David Mazières, a professor of computer science at Stanford University, who is also the chief scientist of the Stellar Development Foundation. The SCP uses a novel mechanism called the Joint Byzantine Protocol to ensure that updates to the distributed ledger are accurate and reliable. SCP has also carried out practical deployment through the Stellar blockchain that has been running since 2015.

When comparing existing consistency algorithms (from transaction recording to distributed classification process), the Stellar consistency protocol has become the main solution supporting user-friendly, mobile-first inheritance. The stellar consensus protocol (starConsensusProtocol, SCP) is a new mechanism called federated byzantine agreement used by Stanford Scp to ensure that distributed ledger updates are accurate and credible. It is also deployed in practice through the Stellar blockchain, which has been running since 2015.

Introduction to the Consistency AlgorithmBefore introducing the zs consensus algorithm, first briefly explain the role of the consistency algorithm on the blockchain, and what are commonly used in today's blockchain protocols. For clarity, this section explicitly uses too many simplifications. Written and incompletely stated. For greater accuracy, see the SCP Adaptation section below, and read the main consensus protocol document.

The blockchain is a fault-tolerant distributed system with a completely completely ordered list of transaction blocks. Fault-tolerant distributed systems are an area of computer science that has been studied for decades. They are called distributed systems because they do not have a centralized server or consist of a decentralized list of computers (referred to as references or peers) that need to agree on the content of the block and the overall implementation. They are also called fault-tolerant routines because they may tolerate some degree of faulty routines in the system (for example, more than 33% of interrupts may go wrong and the entire system continues to operate normally).

Consensus algorithms are divided into two categories: algorithms that elect a node to be the leader of the next block, and consensus algorithms that have no clear leader but all nodes agree on the next block after voting exchange. Send computer messages to each other. (Strictly speaking, the last sentence contains multiple errors, but helps us explain a wide range of strokes.)

There are two main categories of consensus algorithms: leaders, but all agree on the content of the next block by passing computer messages. (Strictly speaking, the last sentence contains multiple errors, but it helps us explain the substance.)

Bitcoin uses the first type of consensus algorithm: all Bitcoin nodes compete with each other when solving crypto graphic challenges. Because the solution is found randomly, the node that first finds the solution will be selected as the person responsible for the round that generates the next block. This algorithm is called "proof of work" and causes a lot of energy consumption.

Bitcoin uses the first consensus algorithm: all Bitcoin converters compete with each other in solving crypto graphic challenges. Find a summary of the algorithm and, by accident, be elected as the leader of the round that produces the next block. This algorithm is called "proof of work" and causes a lot of energy consumption.

zs uses other types of consensus algorithms and is based on Stellar Consensus Protocol (SCP) and a Federal Byzantine Agreement (FBA) algorithm. There is no waste of energy in these algorithms, but they need to exchange a lot of network messages and step on to reach a "consensus" about what the next block should be. Each routine can independently determine whether a transaction is valid, such as determining permissions for conversion and reassignment based on crypto graphic signatures and transaction history. However, for a computer network, to agree to record the transactions and the order of these transactions and blocks in a block, they need to send messages to each other and conduct multiple rounds of voting to achieve consensus. Intuitively, the information from different computers on the network about the next block being one of them looks like this: I admit that we all vote for block a to become the next block ";" I vote for block a to become the next block " ; "I confirm that the majority of shareholders I trust also voted for block a." From this consensus algorithm, the analyst can conclude: "a is the next block; no block other than a is the next block." A major representative of this algorithm is called the "Block" of General Byzantium; although the voting steps above look a lot, the internet is fast enough and this information is lightweight, so the only proof that this consensus algorithm works. Problem algorithm. Some of today's top blockchains are BFT-based variants such as NEO and Ripple.

A major criticism of BFT is that it has a concentration point: because it involves voting, the set of nodes participating in the voting "arbitration" is determined centrally by the creator of the system at the beginning. The contribution of FBA is that each node will set its own "arbitration slice" instead of a centrally determined arbitration, thus forming different arbitrations. New nodes can join the network in a decentralized way: they claim nodes that they trust, and convince other nodes to trust them, but they don't convince any central authority.

A major criticism of BFT is that it has a concentration point: because it involves voting, the set of routines that participate in voting "quorum" is initially determined by the creator of the system. Fba's contribution is that each participant has its own quorum group, rather than a centrally-determined quorum, which will form a different quarter. New routines can join the network in a decentralized manner: they declare a copy of their trust and convince other alert trusts, but they do not need to convince any central authority.

Scp is an example of FBA. Unlike Bitcoin's Proof of Work consensus algorithm, which consumes energy, the SCP protects shared records by guaranteeing that other routines in the network are trusted. Each generated quorumslice in the network, the quorumslice is composed of a quorum group of members of the network, and the validator will only accept new transactions if and only if the part of the quorum also accepts transactions. As a whole you can learn more about the Stellar Consistency Protocol by watching this 7 minute change explanation video or viewing the technical summary of the SCP.

zs consensus on stellar

Protocol (SCP) adaptation

zs's adaptation to the Stellar Consensus Protocol (SCP) The zs consensus algorithm is built on the SCP. SCP has been officially certified [Mazieres 2015] and is currently implemented in the Stellar Network. Unlike the Stellar Network, which is primarily comprised of companies and institutions (such as IBM) as nodes, zs is designed to allow personal devices to contribute and receive rewards at the protocol level, including mobile phones, laptops, and computers. The following is an introduction to how zs applies SCP to personal mining.

The zs consensus algorithm is based on SCP. Scp has been officially certified [Mazieres2015] and is currently being implemented in the Stellar network. Unlike StellarNetwork, which is mainly composed of companies and institutions (such as IBM), zs intends to allow personal devices to introduce the zs application of SCPs to personal mining below the protocol scale.

As a zs miner, zs users can play four roles. which is:
• pioneer. They exist. They can also open an application to request a transaction (e.g. pay another lead company with zs)

• Contributors. The user of the zs mobile app contributes by providing a list of pioneers he or she knows and trusts. . Overall, zs contributors will build a mutual trust graph.

•ambassador. Users of the zs mobile app are introducing other users to zstoken.

•ambassador. A user of a zs mobile application who is dating other users on the zs network.

•Upstream. A pioneer using zs mobile applications, a contributor, and running zs processor software on their desktop or laptop. The zs router software is software that runs the core SCP algorithm. This software refers to the trust provided by the contributors.

Users can play multiple roles as described above. All characters are necessary, so all characters will get new zs coins on a daily basis, as long as they participate and contribute on that day. In the loose definition of "miner", "miner" refers to the user who received new coins as a reward for contribution. All four roles are considered to be that our definition of "mining" is more consistent than the traditional "executive work proof" "Algorithms" are more general, such as in Bitcoin or Ethernet.

node

For readability, we define what a properly connected node is as an SCP file and what it means as a complete node. Similarly, for readability, we define the set of all complete nodes in the zs network as the main zs network. The main task of each node is to configure it to properly connect to the main zs network. Intuitively, a node that is not properly connected to the main network is similar to Bitcoin that is not connected to the main bitcoin network. We define the main zs network as the set of all complete routines in the zs network. The main task of each routine is to configure to properly connect to the main zs network. Obviously, an example of an incorrect connection to the main network is similar to a Bitcoin router that is not connected to the main Bitcoin network.

In SCP terminology, for a node to connect properly means that the node must choose an "arbitration slice" so that all final arbitration including the node intersects with the arbitration of the existing network. More precisely, if the result is a system N 'of n + 1 nodes (v1, v2, ..., vn), then node vn + 1 is correctly connected to n nodes (v1, v2, ..., vn) that have been correctly connected Main network N. +1) Enjoy quorum intersection. In other words, if any two arbitrations of N 'share a node, N' enjoys the intersection of arbitrations. -All quorums U1 and U2, $U1 \cap U2 \neq \varnothing$.
In SCP terms, the correct connection of a node means that the node must choose a "quantum group" so that all the generated quantums containing this node intersect with the quantum of the existing network. More precisely, a router vn + 1 is correctly connected to a main network n with n connected routines (v1, v2, ..., vn). v2, ..., vn + 1) Quantum intersection of copyright. In other words, n 'copyright the quantum link right if and only if any two of its quantums share a capacitor. – That is, for all quantum sets U1 and U2, the intersection of U1 and U2 ≠ any value.

The main contribution of zs to the existing Stellar consensus deployment is that it introduces the concept of a trust graph provided by zs contributors as information that a zs node can use when setting its configuration to connect to the main zs network.
For existing stellar consensus deployments, the main contribution of zs is to date the

concept of a trust graph provided by zs contributors as information that can be used by zs routines when setting up the configuration connected to the main zs network.

In choosing their quorum slice, these nodes must consider the trust graph provided by the contributors, including their own security circle. To help make this decision, we intend to provide auxiliary graph analysis software to help users running Nodes make the best possible decision. The software's daily output will include:

When selecting their groups to be accessed, these variables must take into account the trust graph provided by the contributors, including their own security circle. To assist in this decision, we intend to provide auxiliary graphical analysis software, with routine output from the software including:

- Sorted list of nodes, sorted by their distance from the current node in the trust graph.

Node ranking list based on node page ranking analysis in trust graph

- A sorted list of nodes whose trust graph is sorted by the distance of the routine from the current node;

The list of nodes reported by the community has failed in any way, a list of new nodes trying to join the network

- A list of errors reported by the community in any way A new list of joining the network

- A list of recent articles on the keyword "abnormal zs representatives" and other related keywords;

Multidimensional visual representation of zs network similar to StellarBeat Quorum Monitor [source code].

- quoquoexplorer.com [source] The quorum browser.

- A single StellarBeat Quorum monitor simulation tool that shows the impact of the expected results on the routine's connection to the zs network when the configuration of the current instance changes.

An interesting research question for future work is to develop algorithms that can consider trust graphs and suggest an optimal configuration for each instance, or even set the configuration automatically. In the first deployment of the zs network, when users running Node can update their Node configuration at any time, the system will prompt them to confirm their configuration every day and ask them to update when they think it is appropriate.

Mobile application users

When pioneers need to confirm that a given transaction has been executed (for example, they have received zs), they open a mobile application. At that time, the mobile application was connected to one or more nodes to query whether the transaction was recorded in the ledger and get the latest block number and hash value of the block. If the Pioneer is also running a node, the mobile application will connect to the Pioneer's own node. If Pioneer is not running one node, the application will connect to multiple nodes and cross-check this information. Pioneers will be able to choose the nodes they want their applications to connect to. But to make it simple for most users, the application should have a reasonable default set of nodes, such as the number of nodes closest to the user based on the trust graph, and randomly selected nodes with higher page rank.

When Pioneers need to confirm that a given transaction has been executed, they will open the mobile app. At this point, the mobile application is connected to one or more check boxes to query whether the transaction has been recorded. If Pioneer also runs a node, then the mobile application will connect to Pioneer's own router. If Pioneer is not running a processor, then the application will connect to it, but for the simplicity of most users, the application should have a reasonable alternating arrangement, such as some closest user-based routines based on a trust graph, and random Selected advanced page ranking.

Mining rewards

A beautiful feature of the SCP algorithm is that it is more versatile than the blockchain. It coordinates the consensus of the entire distributed node system. This means that the same core algorithm is not only used to record new transactions in new blocks every few seconds, but can also be used to run more complex calculations periodically. For example, once a week, Stellar Networks uses it to calculate inflation on the Stellar Network and distributes newly minted coins proportionally to all stellar coin holders (Stellar's coin is called lumens). In a similar manner, the zs network uses SCP once a day to calculate the new zs distribution of the entire network among all zs miners (pioneers, contributors, ambassadors, nodes) that actively participate in the day. Put another way,

One of the superior characteristics of the Scp algorithm is that it is more versatile than the blockchain. It coordinates the consistency of the entire distributed asynchronous system. This means that the same core algorithm is used to record new transactions in new blocks every few seconds. For example, the Stellar Network uses it once a week to calculate the expansion on the Stellar Network and becomes a newly minted token that is distributed proportionally. To all stellar holders (stellar

coins are called lumens). Similarly, the zs network uses SCP once a day to calculate the distribution of all zs miners (pioneers, contributors, ambassadors, enums) owning new zs coins. In other words, the zs coin harvest reward calculation is only done once a day, not in every block of the chain.
In contrast, Bitcoin allocates harvest rewards on each block and divides them into all rewards for those miners who are lucky enough to solve computationally intensive random tasks. As a result, only one miner can get 12.5 bitcoins every 10 minutes (about to solve this problem, bitcoin miners are organized in a centralized mining pool, these have improved processing power and increased the rewards. The mining pool is only centralized And their operators are cut down, reducing the amount paid to individual miners. In zs, there is no need to mine resources, because each contributor gets a new zs coin allocation every day.
transaction fee

Similar to Bitcoin transactions, fees in the zs network are optional. Each block has a certain limit on how many transactions it can contain. When there is no backlog of transactions, transactions are often free. However, if there are more transactions, the node sorts them by fee, with the highest fee transaction at the top, and only selects the top transactions to be included in the generated block. This makes it an open market. Implementation: Prorate the costs among the nodes on a daily basis. On each block, the cost of each transaction is transferred to a temporary wallet and distributed from the end of the day to the active miners of the day. This wallet has an unknown private key.

Similar to Bitcoin transactions, charging in the zs network is optional. Each block has a certain limit on the number of transactions it contains. When transactions are not backlogged, transactions are often free. However, if there are more transactions, they are sorted in order according to the charging order, with the highest paid transaction at the highest end, and only the highest transaction to be included in the generation block is selected. This makes it an open market. How to do it: Prorate the expenses once a day between the counts. In each block, the cost of each transaction will be transferred to a temporary wallet. At the end of the day, the wallet will be allocated to the active miners of the day. This wallet has an unknown private key. With all the above unanimous consents, the agreement itself enforces transactions that come in and out of this wallet, just like it is agreed that new zs coins are minted every day.

Limitation And future work

SCP has been extensively tested as part of the Stellar Network, which is the ninth largest cryptocurrency in the world at the time of writing. This gives us great confidence

zs economic model: balance of scarcity and acquisition

Advantages and disadvantages of the first-generation economic model

One of Bitcoin's most impressive innovations is the combination of its distributed system and economic game theory. The system is combined with economic game theory.

The economic model of Bitcoin is simple. There are only 21 million Bitcoins in circulation control. This number is set in code. Since only 21 million Bitcoins can be circulated among 7.5 billion people worldwide, there are not enough Bitcoins to circulate. This scarcity is one of the most important drivers of Bitcoin's value.

Reduced block reward shown below

The initial Bitcoin block mining reward is half of every 210,000 blocks (approximately every 4 years), and the Bitcoin block reward is 50 Bitcoins. The bonus is now 12.5 coins and will be increased to 6.25 coins by May 2020. The decline in Bitcoin issuance means that even if people's awareness of this currency improves, the number of Bitcoins actually mined will decrease.

Disadvantage

Handstand means imbalance

Bitcoin's reverse distribution model (Bitcoin started with more income and now has more income) is that its distribution is not due to the fact that so many Bitcoins are in the hands of a few early users, and new miners are "burning" more energy In exchange for Bitcoin.

zs economic model design requirements:

- Simple: build an intuitive and transparent model
- Equitable distribution: accessible to most of the world's population
- Scarcity: Create a sense of scarcity to maintain the price of zs without depreciating over time
- Elite Hierarchical income: rewards for establishing and maintaining network contributions
- Elite income: rewarding for establishing and maintaining network contributions

Pi-Game Coin Supply

Token supply

Token Emissions Policy

Token Release Policy

1. Total maximum supply (1 billion maximum supply) = M + R + D

2. • M = total mining reward (mining reward)

3. • R = total reward (1 million pieces, while supplies last)

4. • D = Developer Reward (Developer Reward)

5. J = halving mechanism (halving once every 6 months in 2020, halving every 12 months after 2021)

6.t = Developer reward rate

M-Mining Supply (fixed mining supply based on per person casting)

Mining supply (based on fixed mining supply per person)

In contrast to Bitcoin creating a fixed coin supply for the entire global population, zs creates a fixed supply of zs for each person joining the network (up to the first 100 million participants). In other words, for everyone who joins the zs network, there will be a fixed number of zs in advance. This supply is then released during the member's life cycle, based on the member's level of participation and contribution to cybersecurity.

Similar to Bitcoin's index declining function provided to members during the use period to release the supply. Unlike Bitcoin, which provides a fixed money supply to the global population, zs provides a fixed zs value to everyone who joins the network until the first billion participants. In other words, for each person joining the zs network, a fixed amount of zs coins are generated in advance. Then, based on the member's level of participation and contribution to cybersecurity, release this supply over its life cycle. During the user's life cycle, these supplies are released using a bitcoin's exponential decreasing function.

Recommendation supply (based on a fixed referral reward for everyone and shared and shared referrer and adjudicator rewards)In order to be valuable, money must be widely distributed. In order to motivate this goal, the agreement also generates a fixed number of zs as a referral bonus for recommenders and referees (or parents and offspring). Both parties can mine this shared pool and actively mine throughout their entire life cycle (when both parties share). . Both recommenders and recommenders can take advantage of this pool to avoid developing models so that recommenders can "hunt" their recommenders. The referral bonus is a network-level incentive to develop the zs network, and also encourages active participation among members to ensure the network

D-Developer Rewards Supply

Traditionally, cryptocurrency protocols have identified a fixed supply of coins and have joined the central bank. As the total supply of zs to the gradual increase in rewards for zs developers is to make the incentives of zs contributors and the health of the entire network, the gradual increase in rewards to zs developers is to make the incentives of zs contributors and The health of the entire network. be consistent.

F is a logarithmic decreasing function-early members earn more

Although zs tries to avoid extreme concentration of wealth, the network also tries to reward older members and their contributions with a larger percentage of zs. When networks like zs are established, they tend to provide lower utility for participants. For example, suppose you have the first phone in the world. This will be a great technological innovation, but not very useful. However, as more and more people buy phones, each phone holder will gain more utility from the network. In order to reward people who enter the network at an early date, zs's personal mining rewards and recommendation rewards decrease as the number of people on the network decreases. In other words, a certain number of zs are reserved for each "slot" in the zs network.

Roadmap / Deployment Plan

Phase I-design, distribute, and trust graph bootstrap.

The server runs like a faucet, modeling the behavior of a distributed system, because once it runs it will work normally. At this stage, divided from the stable stage of the main network, improvement of user experience and behavior is feasible and relatively easy. The zs network immediately initiated all mined coin users to migrate to the living network. In other words, in phase 1, all block allocations are scattered in the hands of each coin holder. At this stage, zscoin is not listed on the exchange, and any transaction is not feasible.

Phase II-Testnet Phase II-Testnet

Before launching the main network, Node software will be deployed on the test network. The test network will use the same exact trust graph as the main network, but using the test zs coin. The zs core team will host multiple nodes on the testnet, but will encourage more

Before we start the main network, the node software will be deployed on a test network. The test network will use the exact same trust graph as the main network, but on the test zs coin system. The core team will host multiple nodes on the test network, but will encourage more pioneers to start their own counters on the test network. In fact, in order for any third party to join the main network, it is recommended that they start with the test network. The test network will run in parallel with the zs simulator in the first phase and regular comparisons will be made. For example, the results of the two systems will be compared daily to capture gaps and cracks in the test network. This will allow zs developers to make suggestions and implement repair. After the two systems run completely concurrently, the testnet will reach a state where its results are consistent with the simulator. By that time, when the community feels it is ready, zs will move to the next stage.

Phase III-Mainnet Phase III-Mainnet

When the community believes that the software is ready for operation and has been thoroughly tested on the test network, the official main network of the zs network will be launched. An important detail is that during the transition to the main network, account authentication will be performed to ensure that after that, the distribution system and zs network simulator in stage 1 will be shut down and the system will always run independently. Future updates to the agreement will be provided by the zs developer community and zs' core team and will be proposed by the committee. Their implementation and deployment will be supplemented and supplemented, like any other blockchain. A non-existent central authority will convert the currency into a fully decentralized one. The balance of false or duplicate users will be eliminated. At this stage, zs will log on to the exchange and trade with other currencies.

The project team and consultants have extensive project research, development and investment management experience in the field of fintech (including: large databases, AI artificial intelligence, Internet of Things, blockchain, mining investment construction and operation management, etc.) The team is good at integrating development of emerging technologies with finance and other specific business scenarios. Its core developers are from Australia, the United States and so on.

As an integrated application of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other technologies, blockchain has become a hot topic of discussion in international organizations such as the United Nations, International Monetary Fund, and many governments in recent years. Big investment. At present, the application of blockchain has extended to many fields such as the Internet of Things, intelligent manufacturing, supply chain management, and digital asset trading, which will bring new opportunities for the development of new generation information technologies such as cloud computing, big data, and mobile Internet . Ability to trigger a new round of technological innovation and industrial change.

The blockchain is in the transition period from the initial development to individual applications. Some typical applications have already been presented, and they have also shown broad prospects in the financial industry and the commodity industry. The application scope can be roughly carried out from three links before, during and after the transaction. Differentiating, pre-transaction links, including knowing customers, anti-money laundering, information disclosure, etc .; mid-transaction links, including the issuance and transfer of stocks, bonds, collective debt instruments, derivatives; post-transaction links, including registration, depository, clearing, and settlement Income, data sharing, share split, shareholder voting, dividend payment, collateral management, crowdfunding management. At present, countries have different attitudes and regulations on blockchain technology.

Australia's laws and regulations on blockchain. In August 2014, the Australian Taxation Office (ATO) issued the Bitcoin tax guidelines, which officially incorporated Bitcoin and related business activities into the existing tax system. The standard does not consider bitcoin as a currency, nor does it define its financial asset positioning, but treats it as a common asset. The main contents are as follows: personal use of bitcoin transactions does not involve any taxes, taxes, and income taxes; businesses use bitcoin to buy goods Or services, you must convert the value of the purchased goods into Australian dollars and record them as business income; capital gains, as an asset, involves capital gains tax when the company cleans up bitcoin; using bitcoin to pay Wages, this type of payment is similar to fringe benefits for an enterprise, and employers may pay fringe benefits for this; income derived from mining (production) of Bitcoin and mining (production) of Bitcoin for business purposes will be considered taxable income.

EU legal restrictions on blockchain On July 5, 2016, the European Commission passed a motion to amend the Fourth Anti-Money Laundering Act (4AMLD), which explicitly included virtual currency transactions in the anti-money laundering framework. In August 2013, Germany recognized the legal status of Bitcoin and included it in the national regulatory system. As a result, Germany became the first country in the world to recognize the legal status of Bitcoin. The German government stated that Bitcoin can be used as a private currency and currency unit Bitcoin is tax-free for personal use for one year, but is taxable for commercial use. The German Financial Supervisory Authority believes that Bitcoin is a value token used to exchange real economic goods or services in a barter club, private market or other payment system. Bitcoin trading platform bitcoin.de has also cooperated with Fidor Bank.

Countries around the world have made laws and regulations adapted to the blockchain industry and the development and supervision of encrypted digital assets according to their national conditions. Blockchain technology is limited by the supervision and control of many different regulatory organizations around the world. Zs may be limited by their requirements or actions, including but not limited to limiting the use of digital tokens. For example, zs may slow down or be affected by Limit zs features or repurchases in the future. Token buyers must conduct due diligence on their own to ensure that they comply with all their local laws related to cryptocurrencies, taxes, bonds and other regulations.

Funds collected during the angel or private placement stages are not covered by insurance. If they are lost or lost value, the buyer may not be able to get any assistance from private or public insurance.

When trading on the open market, the price of cryptocurrencies is usually volatile. Price shocks often occur in the short term. Such price fluctuations may be caused by market forces (including speculation), changes in regulatory policies, technological innovations, the availability of exchanges, and other objective factors. Such fluctuations also reflect changes in the balance of supply and demand. The risk involved in the zs transaction price shall be borne by the zs trader.

Risk of insufficient information disclosure

As of the date of this commercial white paper, zstoken is still in the ecological construction and business development stage. The priority VC direction of its core business will be constantly updated and changed according to the project profit and risk analysis model. Although the white paper contains specific information about zstoken's various ecologically related businesses, it is not absolutely complete, and the zs seller may make adjustments and updates to this information from time to time based on specific purposes. The seller cannot and is not obliged to inform the participants at any time that every detail in the construction of the zstoken ecosystem (including its progress and expected milestones, whether delayed or not), therefore does not necessarily make the participants aware of the zstoken business development Information from time to time. Insufficient information disclosure is inevitable and reasonable.

Disclaimer:

This commercial white paper does not constitute an invitation to purchase zs in any illegal jurisdiction. All or any part of this white paper is neither, nor should it be considered, any form of legal, financial, tax or other professional advice. You should seek independent, professional advice before deciding whether you should buy, sell or collect any zs. You are responsible for the evaluation, assessment and decision making of any purchase, sale or collection of zs. zstoken will not force anyone to accept zs, and to the maximum extent permitted by law, zs will not bear any responsibility for any negative effects or consequences caused by zs.