Shell Chain

The public chain of block chain focus on game development

www.shellchains.com

Contents

一、About shell chain

Shell Chain is a public chain focusing on the development of block chain games. It has high concurrency, low latency, low cost, and high privacy. It will build a game incubation platform based on block chain technology. The decoupling of the block chain can not be modified, and the ideas, developers, players, and advertising service providers are linked openly and transparently, effectively reducing the cost of game development and promotion. At the same time, through the continuous improvement and selection, the high-quality block chain is hatched game.

In the whole shell chain ecology, the Shell Chain Pass is issued, which is circulated in the game platform. Shell acts as a value carrier in the whole ecology and realizes low-cost transmission.

Shell, as a shell chain public chain token, has the following uses and values:

(1) As a Shell transfer fee;

(2) The only evidence of circulation in all game ecosystems that are incubating as a platform for delivering value, such as: purchasing equipment, upgrading levels, normal consumption, etc.

(3) The game developer uses the Shell to pay for the use of the shell chain platform and pays the advertising service provider's promotion fee;

(4) The player earns the shell as income by participating in the game or completing the task;

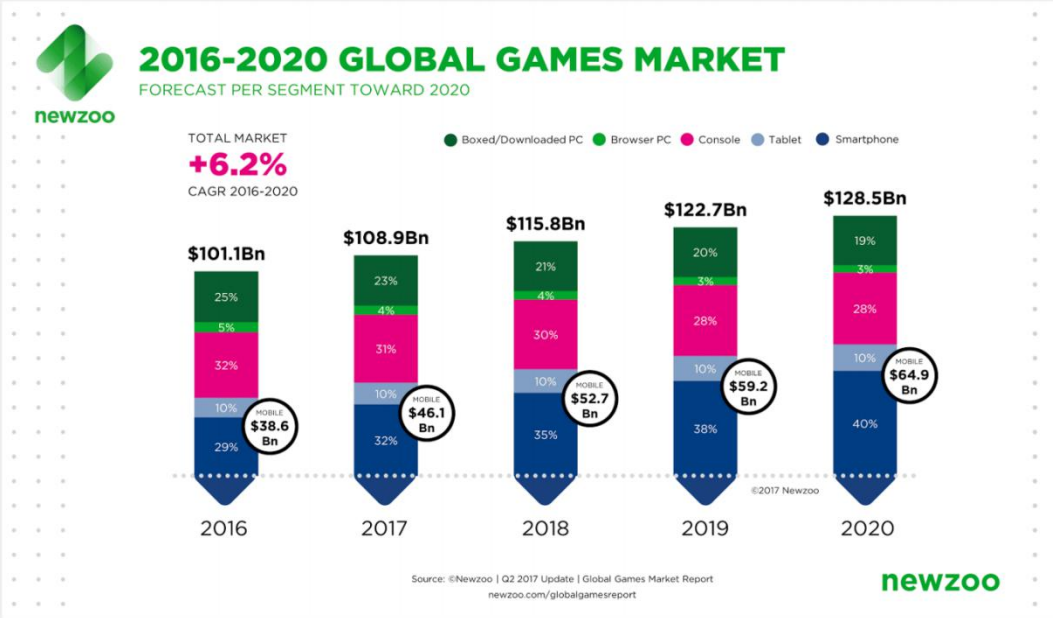
(5) Using the shell chain platform profit, constantly repurchasing and

destroying the Shell, so that the Shell continues to add value.

二、Background of the project

1、Game market size

The global game market is very large. According to Newzoo's latest research, there are 2.3 billion gamers worldwide, contributing $115.8 billion to the game market in 2018. Starting in 2016, the average annual growth rate is $7.35 billion, with an average annual growth rate of 7.2%.The market is expected to grow further from 2019 to 2020, with revenues expected to reach $128.5 billion in 2020.



In the video game market, the current free-to-play model is the mainstream, and its revenue comes from the sale of digital goods. For example, mobile game makers Royale and Clash of Clans created $6.9 billion in sales in 2016, the king of Tencent. Glory earned $1.9 billion in revenue in 2018.Although a large number of

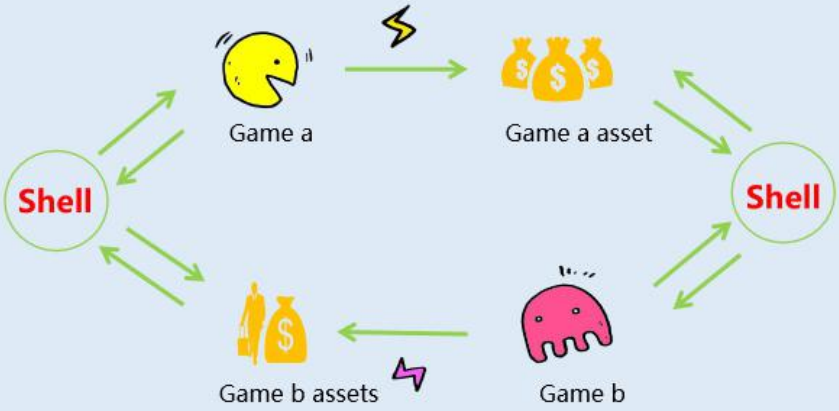
games are currently free, gamers who purchase tens of billions of dollars of game items each year cannot be circulated and cashed.

2、Industry pain points and solutions

(1) Game assets are difficult to realize

The game platform in the market is diverse and cumbersome. Players may spend hundreds or thousands of dollars to unlock mystery boxes and countless hours of playing time to earn rare game merchandise. However, when they finally stop playing the game, the game skin The props and gold coins are difficult to circulate and realize, and the cost and risk of circulation are also extremely high.

The shell chain platform public chain uses the decentralization of block chain, the transparent mechanism of distributed node verification, and the highly efficient tradable asset economy model to unify all the game passes of the platform, and use Shell as the only pass to freely circulate in all games. Realizing low-cost, low-risk game items, and making the game playable, increasing player income, and improving game stickiness.



Shell chain platform game asset circulation diagram

(2) Game fairness is difficult to guarantee

All the data of the traditional game is stored on the centralized server, and the game fairness cannot be guaranteed.All games on the shell chain platform run on block chain smart contracts, which are distributed and cannot be tampered with.Distributed means that the output of the contract is verified by everyone on the network; no tampering means that once a smart contract is created, it can never be changed.In order to prove fairness, the smart contract works by using a non-controllable basic data, combined with a certain formula algorithm, to derive random results, and the results are still random, thus achieving true randomness.

How Shell Chains Guarantee Game Fairness

To ensure game fairness, the platform is completely transparent and verifiable backtrackable.

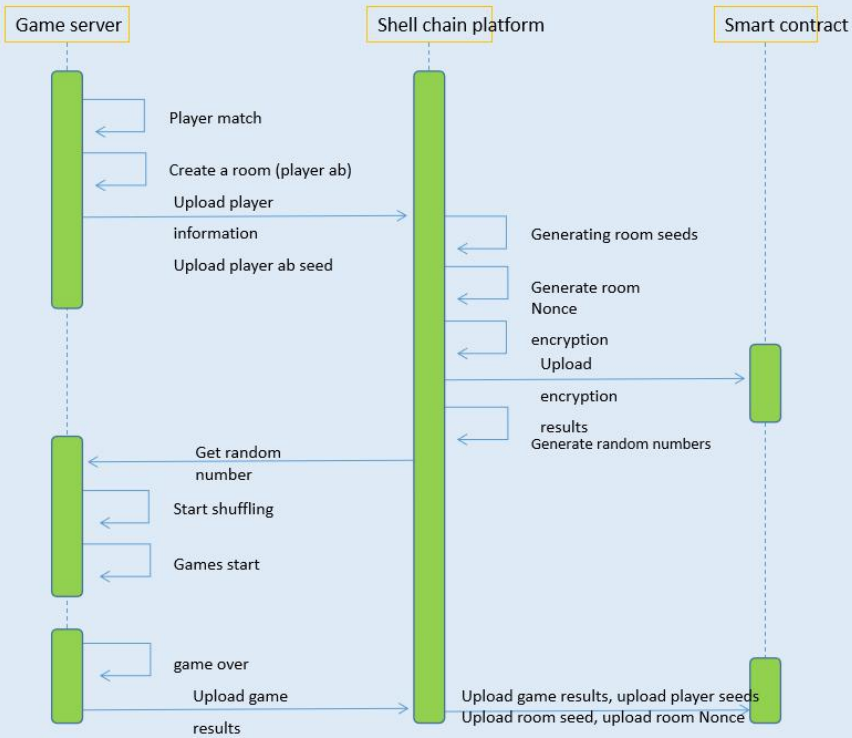
With reference to fairidice's architecture, we offer the following design for game-like games:

- Game preparation

The player uploads the client seed through the game server and prepares the game. After playing the game platform, the balance is checked in the contract, and the shell of each game is prepared to be successful. The player enters the waiting queue of the game server and waits for the server to match the player.

- Dealing order

In order to prove the fairness of the game and ensure the verifiability of the game, three types of parameters are designed to calculate the order of each game: player seed, room seed and room nonce, as shown below:



After the game server matches the good player, the room is created, and the room information and the player seed are uploaded to the shell chain platform; at this time, the game platform generates the room seed and the Nonce, and the

room seed and the nonce are encrypted and uploaded to the area by asymmetric encryption. On the block, this can verify that the room seed and nonce have not been modified after the game is over; then the player seed and the room seed are hashed to determine the order of the cards; after the game is over, we will announce the server seed and the player seed and nonce, the player The order of the cards can be verified by a script.

(3) High development cost

Traditional games have scattered work, repeated development needs, scattered work, and the inability to reuse tokens. As a result, common game development costs and cycles are generally long, making it difficult to cope with the rapidly changing environment of the market.

After the Shell Chain is modularized, after the game's underlying architecture is developed, anyone with a good Idea can develop and customize their own games on the shell chain platform without having to understand the development process. The platform users are both developers and developers. Player.This will greatly reduce the difficulty of game development, and maximize the enthusiasm of the public to create a colorful game world.At the same time, through the growing user base of the shell chain platform, the new game has the most basic users, saving a lot of promotion costs.

(4) Game threshold

The centralized game brings a perfect user experience to the user, but the fairness cannot be guaranteed. The decentralized game can guarantee fairness, but the game experience is difficult to improve, and the threshold for participating in the game is very high and difficult to popularize.The shell chain will look for balance in the centering and decentering, giving users the ultimate user experience.

How does the centralized system participate in block chain games?

The shell chain comes with a centralized user system, similar to a traditional exchange account. The main logic is:

The system has a unified recharge and withdrawal of the Shell account, the user logs in through the mobile phone number, and assigns a UID

The user recharges his UID as a MEMO value in the centralized system. When the user plays the game, the system automatically recharges the DApp game contract with the UID as the MEMO. The contract will be differentiated by the UID. The user needs to mention the funds in the contract. At present, the contract withdraws the user UID as a MEMO to the previous recharge address, which is the centralization system recharge account.

Through the above logic, the centralized account system can be used to call the game contract.

(5) Game privacy

Traditional games, and even most block chain games can't ensure privacy. Shell Chain uses the Anonymous Privacy Policy to make all the information such as game accounts and assets private and completely anonymous.

三、Shell chain platform core value

(1) Through the platform to unify the Shell, to ensure the low-cost and high-efficiency transfer between different game assets, to ensure the ability of customers to achieve liquidity.

(2) Through the Shell Pass, build a complete ecosystem, effectively combine developers, game players, promoters, each person can have a way to earn a Shell pass, you can also use the pass to buy the corresponding services.

(3) Unlike other public chain projects such as ETH, EOS, and wave field, the Shell Chain does not require a token to be issued for each project, resulting in value dispersion.The value of all items in the Shell Chain is concentrated on the shell coin, allowing the Shell to continue to appreciate, and any game uses Shell to pay for circulation to achieve value transfer.Users also do not need to manage tokens for each game because they participate in multiple games.

(4) Balance between decentralized games and centralized games to achieve a centralized user experience and decentralized fairness, while reducing the barriers to block chain games and allowing block chain games to reach the public.

（5） Through modular design, the development details are shielded, so that anyone can release the game on the shell chain platform according to their own ideas, without the need to understand development, to achieve mass innovation, the number and scale of games will usher in a big explosion.Let publishing block chain games be as simple as issuing tokens on eth.

（6） By introducing anonymous currency technology, game privacy is guaranteed, a true anonymous game.

四、Shell chain public chain infrastructure

Shell Chain is a low-level public chain based on graphene 2.0 technology. The network is faster than EOS and can complete broadcast faster. It is suitable for high real-time requirements such as token circulation, high-frequency games and payment industry.V1 version test network, the actual throughput of a single node is up to 3700TPS, and when more miners join, it will reach 100,000 TPS.

The Shell Chain uses the DPOS consensus algorithm and the block generation speed is 0.5-1.5 seconds.The fast update structure of its extended data block can be run using a small server node (mobile phone). Based on its large number of fast-running nodes, it can resist the risk of 51% attack and hard fork. The Shell Chain will It is a new generation of safer block chain systems.

The Onion routing protocol used by the Shell Chain allows users to form tunnels or paths through a distributed network, using multiple nodes as hops to confuse the destination and origin of data packets.The service nodes on the

Shell Chain network will run a low-latency Onion routing protocol to form a fully dispersed overlay network called the Shell Chain network.The network does not rely on trusted authorities, and its state is entirely from the block chain.Users can connect to individual service nodes and create bidirectional paths for packets to be routed.This network can be used to access internal hosting services called SNApps.Users can use the service node exit function to browse the external Internet without exposing their IP.

(1) Low latency anonymous routing protocol (llarp)

The basis of all service node applications is the anonymous routing protocol, which defines how each service node communicates with its peers.Shell Chain proposes a new routing protocol called LLARPIt is designed as a mix between Tor and I2P to provide additional required features compared to any existing routing protocol.LLARP is specifically built to run on top of the Shell Chain service node network, and all LLARP optimizations consider this architecture.To understand the goals of LLARP, it's best to analyze existing routing protocols and consider how LLARP can improve them.

Onion Router (Tor)

In recent years, Tor has been the most popular hybrid network.The Tor network maintains a high level of review resistance and has proven to be a valuable tool for protecting Internet privacy.However, Tor is not a decentralized network, but a layered network.Tor relies on a set of directory permissions,

which are centralized servers operated by a group of volunteers near the Tor Foundation. These directory permissions perform two main functions. First, they act as trusted reporters in the node state in the network. When a Tor user (or relay) connects to the network for the first time, they can connect to one of the ten hard-coded directory permissions that provide a file called a consensus for the user or relay. This file provides the Tor network. A list of all relays, protection nodes, and egress nodes currently running (excluding bridges).Second, the directory organization also measures the bandwidth that each relay can provide to the network. They use this information to classify the relays to determine if the node can function as a relay, protection node, or egress node.

This high concentration has created Tor's vulnerability.In 2014, Tor received a message about a trusted threat to cancel a directory rights server.. If you want to turn off directory permissions in the US and Germany or the Netherlands, it is enough to shut down five of the ten directory permissions servers.This will result in a highly unstable Tor network and a significant reduction in the ability of new relays to interact with the network.The communication method in Tor is also limited because Tor only allows communication via TCP.IP over Tor is possible, but it lacks support for UDP-based protocols such as VoIP.

(2) Invisible Internet Project (i2p)

I2P uses different methods for the mixnet architecture to maintain a higher level of trust agility by referencing a distributed hash table (DHT) to determine

network state rather than trusted directory permissions.. I2P also allows TCP and UDP traffic to support a wider range of protocol interactions.However, I2P does not have a stable development process, and it has accumulated technical problems over time, especially in its encryption use, I2P uses 2048-bit ElGamal, compared with elliptic curve operation, encryption and decryption speed slow.Although there are plans to move away from ElGamal in the I2P roadmap, progress has been slow.

In addition, I2P lacks formal support for exit nodes, which means that most of the traffic on the network is accessing internally hosted websites called Eepsites.This greatly reduces the main purpose of the I2P network to reach an anonymous network, the purpose of which is to access the wider Internet.

Again, the way i2p is built means that most users connected to the network also become routers, which is problematic because the resulting network usually lacks enough bandwidth to build fast paths.The network speed in a hybrid network is bottlenecked by the least functional nodes in each circuit, and since low-performance users become relays in i2p, overall performance degradation can be seen.

Finally, I2P differs from Tor in that it provides packet switched (rather than circuit switched) networks.Instead of establishing a single long-term tunnel through which all traffic passes, I2P establishes multiple paths, and each transmitted packet can be used to route different routes through the network.This

enables I2P to transparently bypass network congestion and node failure.

N2P and Tor did not completely mitigate the Sybil attack.An attacker with sufficient motivation and sufficient time to purchase a large number of relays can perform a time analysis that disrupts user privacy.The effectiveness of this analysis increases the number of exit nodes, relays, and protection nodes that the attacker operates on.. Tor and I2P are completely operated by volunteers who donate time and money to the node's operations.We speculate that networks built with financial incentives rather than altruism can achieve greater resistance to attacks while providing more reliable services.

LLARP

Ralp runs without the need to use directory permissions, but instead relies on dht built through block chain tag transactions, which allows the service node to act as a router in the network.Dht does not monitor or record bandwidth.Instead, bandwidth measurements and classifications are generated by groups that evaluate each node and determine if it can provide the appropriate bandwidth.

In the Open Systems Interconnection Model (osi model), llarp only attempts to provide an anonymous network layer.This means it supports a wider range of Internet protocols and can also minimize the overhead of storing file descriptors if the exit node passes the User Datagram Protocol (udp).traffic. In addition, LLARP chooses packet-switched routing instead of tunnel-based routing,

allowing for better load balancing and network redundancy.End users of the Shell Chain network do not expect (or even allow) routing packets, which means that the Shell Chain network exposes itself to the much lower attack surface of the Sybil attack due to the large capital expenditures required to begin service node operations.

(3) Shell Chain Service

Similar to the investment in miners' hardware, each service node operator freezes the Shell Chain when it starts operating the service node.This frozen capital has two purposes.

1. Each service node operator has a great influence on the success of the network.If any service node operator provides poor performance or dishonesty for the network, they risk the risk of depreciating their own interests.

2. It provides an opportunity for more active law enforcement, and if the network can effectively limit dishonest nodes from receiving rewards, then the dishonest node must bear the opportunity cost of reward losses and remaining lock-up time on the collateral.

If we believe that the above ideas are correct and we can enforce penalties on underperforming nodes, then we can create service node groups that can be queried to reach consensus on the state of the block chain or enforce special Off-chain node behavior.In the Shell Chain, this behavior is related to network

and storage activities.These off-chain activities are combined to become the back end of user-oriented applications that take advantage of these ideal attributes, called Shell Chain services.

(3.1) Shell Chain message

The first Shell Chain service developed and deployed on the Shell Chain network will be a distributed end-to-end encrypted private messaging application called Shell Chain Messenger.

End-to-end encrypted messaging applications provide users with a platform to send messages without displaying their content, but they rely on centralized servers that can be located, blocked, and closed.. These centralized service models pose a high risk to the anonymity of the communicating parties because they often require users to register phone numbers or other identifying information and connect directly through the user's IP address.This information can be extracted from the server through data leakage or legal processes and used by the user.Using the service node architecture on the Shell Chain network, we can provide services similar to popular centralized encrypted messaging applications (such as Signal) with higher privacy capabilities.

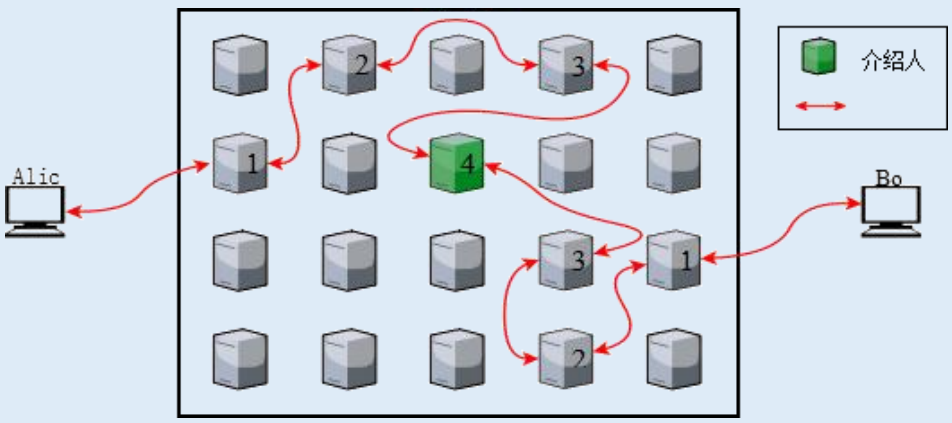
(3.2) Message routing

Message routing on the Shell Chain network varies depending on whether the receiving user is online or offline.When both users are online, higher

bandwidth communication is possible because the messages do not need to be stored on the service node.In the Shell Chain, the public key acts both as a long-term encryption key and as a routing address.In the simplest case, this key should be exchanged out of band to ensure protection against man-in-the-middle attacks.This exchange should be carried out through another secure exchange.

(3.3) Online news

Once Alice knows the Bobs public key, she thinks he is online and tries to create a path to him.Alice does this by querying the DHT of any service node and obtaining any imported sets corresponding to the Bobs public key.In LLARP, the introduction set lists the introducers maintained by each user.The path can be established by these introducers.Through Bobs introducer, Alice now selects three random service nodes as the intermediate hop (introducer) between her departure and destination.A path has now been established through which Alice and Bob can transmit messages.If certified and using OTR, Alice and Bob can now communicate while maintaining a high level of privacy.

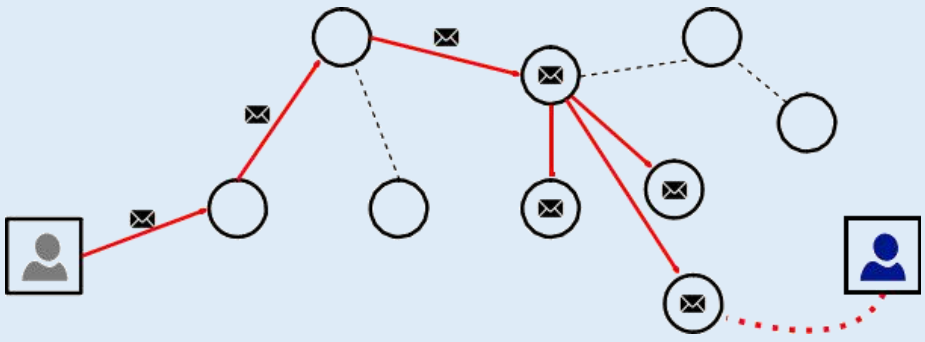


Shell Chain network service node

F*igure 1: A simplified version of the online route that Alice communicates with Bob, using a random service node to establish a path through the network.*

(3.4) Offline messages

If Alice fails to receive Bob's response, she can initiate an offline messaging process.Offline routing uses a modified version of the postal service on the flood (PSS). A flood is a logical grouping of service nodes based on their public key and the hash of the block in which their staking transaction first appeared.Each flood has a flood ID consisting of 9 nodes.In order to send a message to Bob, Alice can use his public key to calculate the group to which Bob belongs.Using this information, Alice can anonymously route messages through the network to random service nodes in the group.When a serving node receives a unique message to its flood, it must distribute the message to the other eight nodes in the flood.In addition, all nodes are required to store their assigned time-to-live (TTL) messages.When Bob goes online, he can query any two nodes in his group to find messages he can decrypt.Protect offline messaging from spam by small work proof attached to each message.



F*igure 2: Alice sends a message to Bob, Bobs allocates a flood to B, and when*

Bob goes online, he queries the random nodes in his group and receives the Alices message.

(4) message encryption and authentication

Once the message chain is established, Shell Chain Messenger enforces Perfect Forward Secrecy (PFS) and Deniable Authentication (DA).PFS and DA are key concepts of the Off The Record (OTR) messaging protocol. Centralized services such as Signal and WhatsApp use encryption that maintains OTR protection.Shell Chain models its OTR implementation based on the existing Tox protocol, a distributed peer-to-peer instant messaging protocol that uses a highly audited NaCl library.

PFS protects against long-term key exposure attacks.Each session uses a new shared encryption key, so if a single session key is displayed, the entire message chain is not destroyed.If a third party wants to crack the encryption of the message chain, you need to get the key for each session.Compared to existing methods, PFS ensures that Shell Chain Messenger is extremely difficult to compromise, such as Pretty Good Privacy (PGP) encryption, which requires only one long-term key pair to destroy the entire message chain.

Da refers to the ability of both parties to prove each other that they are the sender of each new message.However, third parties cannot determine who the true sender of any message is.When da is used, a message authentication code (mac) is issued after each session, allowing third parties to reasonably create messages that

appear to come from the sender's public address.Once properly implemented, no third party can prove that the sender of a particular message is the actual sender.

(5) User authentication

User authentication is very important to ensure protection against man-in-the-middle attacks.For example, if Bob expects a message from Alice but doesn't know what her public key is, then the third party (Eve) can pretend that Bob is sending a message to Alice.This is why users should verify each other before sharing personal information.

Like Pidgin and other OTR messaging services, Shell Chain Messenger uses Pre-Shared Key (PSK) authentication.Users have multiple options to build a PSK.They can create an out-of-band key, or they can agree on PSK through Shell Chain Messenger and ask another question, no third party knows the answer.Shell Chain will implement PSK authentication based on a modified version of the Pidgin encryption authentication plugin.

(6) SNApps (service node application)

The functionality of SNApps is similar to the so-called hidden services in Tor, which have thrived.They provide users with a way to fully interact in a mixnet environment, providing a higher degree of anonymity than accessing externally hosted content.SNApps allows users to set up and host markets, forums, reporting sites, social media and most other Internet applications on their own

machines or servers while maintaining full server and client side anonymity.This greatly expands the reach of the network and allows users to build meaningful communities within the Shell Chain network.

The SNApp operator uses the traditional server-client model, the main difference being that the service node will become a middleman in the user connection through the Shell Chain network.When SNApp wants to register on the network, it must update the DHT with its descriptor.The descriptor contains various importers, which are specific service nodes that the user can contact to form the SNApp path.Once these paths are set, users can connect to the SNApp without requiring either party to know where the other party is on the network.

(7) Exit node

The exit node allows users to make requests to the wider Internet and return them via the mixnet.If used correctly, the exit node allows the user to browse the Internet privately without exposing the user's IP address to the server.While exiting a node is critical to the Shell Chain extension utility, it can be harmful to force all service node operators to act as exit nodes.Being an exit node can expose the operator to legal risks because users who exit the node may perform malicious activities when they use it as a proxy.Since the egress node simply relays traffic from the Internet to the end user, the egress node typically receives a Digital Millennium Copyright Act (DMCA) request or is often considered a source of hacking.While in most jurisdictions, secure harboring laws may protect

egress node operators, Internet service providers that carry service node traffic on their servers may be concerned about legal risks and often cut off services to exit nodes.

At startup, the service node is assigned a relay flag and is limited to routing packets within the Shell Chain network, but never makes requests to the wider Internet.If the operator wants to be an exit node, they must choose to join, so they will show an understanding of the additional risks and also submit additional torrent tests.

When selected as a block reward, the selection as an exit node provides the operator with a double normal reward for the relay.This incentive is provided to ensure that the exit node operator has sufficient financial incentives to operate the exit node, thereby helping to prevent Sybil attacks specifically for taking over the exit node network.This is a vulnerability that Tor suffers due to the low ratio of exit nodes to relays.

(8) Remote node

In any given cryptocurrency network, a complete copy of the block chain is not possible or practical for many users.In Bitcoin and Ethereum, users can choose to connect to a public full node that contains a copy of the block chain and can query and submit transactions to the network.This is effective because Bitcoin and Ethereum complete nodes can efficiently search for transactions in the block chain that target the user's public key.

Due to the construction of the CryptoNote currency, public intact nodes (called remote nodes) are under greater pressure.When users connect to remote nodes, they must temporarily download each block (when creating a wallet or from the last checked block) to their local machine and check each transaction to find a public that can be generated from the user's private view key. Transaction key.This process can have a significant performance impact on remote nodes.Considering that this service has no rewards, it can prevent users from running synchronization services for light clients.CryptoNote mobile wallets are often unreliable and sometimes have to switch between remote nodes multiple times before establishing a reliable connection to scan block chains or commit transactions.

In addition, a malicious remote node operator running one of the few popular nodes can record the user's IP address when broadcasting a particular transaction.Although this attack does not reveal information about the actual transaction, a specific IP address can be associated with the transaction and can then be used to establish a link to a real-world identity, thereby jeopardizing privacy.

Shell Chain circumvents these problems by requiring each service node to act as a remote node that can be used by normal users.Service nodes are naturally suitable for this work because they already have a complete copy of the block chain and form a widely distributed network of high-bandwidth nodes.By using a service node as a remote node, there are inherent financial limitations on

how many remote node networks a given party can have and therefore how much data the malicious node operator can collect.

(9) CryptoNote correction

The Shell Chain is functionally similar to its companion CryptoNote currency.However, in addition to adding service nodes and their associated related features, there are some key differences.

(10) asic barrier

An application specific integrated circuit (asic) is a computer chip built for a single function.In a mining environment, asic is used to compute a specific hashing algorithm.They pose a risk to decentralization because they exceed all other mining methods, are manufactured by specific companies, have very limited distribution channels due to the specialized nature of the hardware, and they require significant capital costs to develop and operate profitable.Asic has potential benefits, such as the capital cost requirements that miners must bear to invest in algorithm-specific hardware, which makes them less likely to act in a way that undermines their investment.However, the distribution and manufacture of asic chips with mature hashing algorithms is still concentrated in a few large companies.These companies can refuse to ship to certain regions, determine which regions and customers get the best performance asic, they can build limited operating and manipulating prices.

To prevent ASIC miners from monopolizing network hashes, many cryptocurrencies have developed ASIC-resistant hashing algorithms such as Scrypt and Ethash.. Until recently, Monroe also used the CryptoNight hash algorithm, which requires a large amount of L3 cache to run.In theory, due to the high memory requirements, this should make it difficult to produce ASIC chips.However, in 2018, Bitmain released X3, a CryptoNight-specific ASIC that can mine at ten times the speed of a graphics processing unit (GPU).. Other hashing algorithms have suffered a similar fate, and Scrypt, Ethash and Equihash are now being exploited by ASICs.

In order to combat the use of ASIC, Monroe has proposed a hard fork strategy every 3-6 months to slightly change the CryptoNight hash algorithm (the first branch is transferred to CryptoNightV7)). The capital and time required to build an asic is very important, and with a highly specific hardware design, slight adjustments in the hashing algorithm can invalidate the chip design, wasting time and capital investment by the asic manufacturer.However, this approach introduces its own problems.If the changes made to the algorithm are not sufficient to prevent asic from reprogramming, the network may become vulnerable to centralization of hash values until another hard fork is possible.This should also be the case with field programmable gate arrays (fpga).

It can be considered in the asic resistance strategy, where infrequent small changes in the hash algorithm can be easily reprogrammed into fpga.Another issue is the possibility of periodic changes to the core consensus mechanism that can lead to unexpected errors, and it is common to focus on developing

such changes around the core developer team.

A number of alternative work proof algorithms have been proposed to periodically address the need for hard forks, including verifiable memory hard hash algorithms such as Argon2, Balloon hash, and polymorphic hashing algorithms such as ProgPoW and RandProg.The Shell Chain team will release more research on the above algorithms to develop long-term solutions for ASICs.

In parallel with this work, Shell Chain will incorporate a version of CryptoNight called Cryp-toNight Heavy, which maintains ASIC resistance to CryptoNight ASIC miners.Cryp-toNight Heavy differs from CryptoNight V7 in many ways: it increases the scratchpad size to 4mb and changes the way in which implosions and explosions are handled. These changes make it different from the largest ASIC miner target (Monroco's CryptoNight V7) and provide more robust ASIC development protection before a more permanent solution.

(11) Dynamic block size

Shell Chain does not have a fixed block size. Instead, the block size changes over time and grows as the network reaches higher transaction throughput to include more transaction Shell Chain block sizes by observing the last 100 blocks. The middle block size is scaled and the maximum size of any new block is slowly repositioned accordingly.

The long-term problem with other cryptocurrencies is that large chunk sizes

put a burden on the nodes that store and verify transactions.As the block size increases, nodes running on lower level hardware cannot process and propagate new blocks, causing the node network to be concentrated in network of nodes that have commercial benefits to the maintenance node.This can be worrying because distributing the block chain over many nodes allows the state of the chain to be confirmed between many different parties, thereby increasing its effectiveness and reviewing resistance.

In the Shell Chain, a portion of the block reward is provided to the service node, which processes and propagates the block as a complete node.Because the service nodes with insufficient bandwidth and performance are removed from the service node network (see 7.3), the reward pool performs its own minimum performance requirements.The incentive structure not only ensures that the number of nodes remains high, but that the nodes have sufficient performance levels to successfully share block chain data on the network regardless of the block chain size or bandwidth requirements.Even so, transaction size optimization is still needed to ensure that the network is effectively scaled up to keep the service node's operating costs down, so that high node counts can be maintained over the long term.

(12) Ring signature size

Ring signatures are used to hide the actual output in any given transaction.The size of the ring signature refers to the number of mixtures used

to construct the loop.Monroe currently has a mandatory minimum ring signature size of 7, of which 6 mixins are used with the real unused output in the transaction.

However, in article 0001 (published by the Monroe Research Laboratory), the effects of larger ring sizes were sparsely studied, and the effects of different ring sizes were analyzed, while attackers with large outputs on the block chain. It turns out that a higher ring size reduces the time range in which a malicious attacker with a large amount of unspent output can perform an effective transaction analysis.Requiring larger ring sizes also prevents theoretical attacks known as EABE / Knacc attacks, Third parties (ie exchanges) can perform limited time analysis of transactions between two users.

In addition, Monroe has no maximum ring size enforced by network consensus rules.Many wallets, such as the Monroe gui wallet, have a ring size of 26.However, users are free to manually create transactions for any ring size they wish, as long as it is higher than the ring size of 7.This is problematic because most wallets have a default ring size of 7.Increasing the transaction ring size to more than 7 will make it stand out.In addition, if the individual transaction always uses a non-standard ring size in Monroe, the passive third party can use time analysis to analyze the block chain and infer the pattern.

Transfer hash	Ring size	TX size [kB]
3feaff3f48de0bc4c92ec0272ec027b6433f404aca8212c1215c1215e945697	7	13.47
39d44f7c0a2e8f3823a51456d7b0bf269171c4582e054c55e95e95cad0	7	13.47

e08f5a937e7711d 440353394e98 dcca32749dda231c56d1278d49c0a231	7	13.5
ab35e69d9cc29c9129c90d8b8b7ab7ab454c82127f d76357f766387	7	13.5
6d8ccd56dc2d3d3d3d7eb7de03ba70d4d4f4f42e9f16d6b8b02229c272	10	13.87

Figure 3: Shows how non-standard ring sizes stand out

Shell Chain improves these two problems by statically forcing ring-size and ring-size to 10.Statically setting the maximum ring size protects users with more than 9 mixins in the construction ring and sets the minimum ring size to 10, which can effectively prevent the attacker from having a large number of outputs from identifying the true output in the ring signature.The larger ring size also non-linearly increases the default agitation effect and becomes more effective as the ring size increases.

In the current trading scenario, increasing the ring size to 10 will result in a 2.6% increase in transaction size.However, when the anti-ballistic measures are implemented, it will increase the transaction size by about 8-13%.This is because Bulletproofs has led to a reduction in the overall size of the transaction.Increasing the minimum ring size can increase problems in networks that lack an architecture that supports larger transactions due to increased overhead.However, in the Shell Chain, this burden can be carried by a service node that provides sufficient bandwidth.

五、Token issue

The Shell Chain platform will release the platform coin based on the ERC20

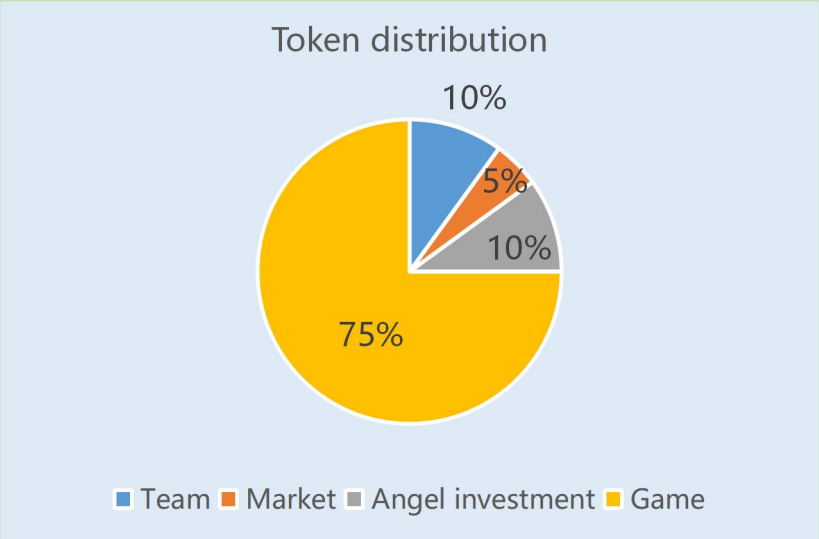
standard, with a total of 2.1 billion copies. After the main online line, the shell will be replaced by a 1:1 ratio for the shell based on the shell chain.

(1) 10% Shell tokens, totaling 210 million pieces, owned by the operation team, released 30% in the first year, and released linearly in December of the following year;

(2) 5% Shell tokens, a total of 105 million, marketing activities and gifts;

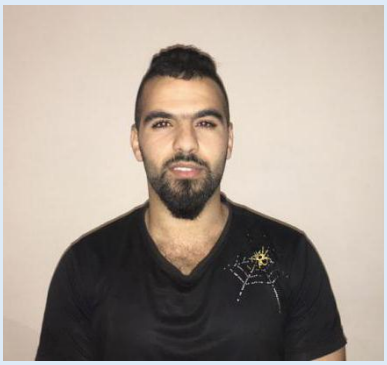
(3) 10% Shell tokens, a total of 210 million, angel fund investment income, released 20% after three months on the line, and then released 10% per month;

(4) 75% Shell tokens, a total of 1.575 billion, used for game eco contributor rewards.



六、team introduction

The Shell Chain team consists of top game industry veterans, technology innovators and proven personnel. To highlight some of the team's qualifications and experience, the details are as follows:



Abner

CEO

In 2012, he began to contact Bitcoin and began to conduct in-depth research on Bitcoin and block chain. He is a decentralized and determined believer. The leadership team has developed several block chain games in ETH and EOS, and has deepened the block chain game. Research, fully understand the current state of the game field, and always look for solutions, first proposed the concept of decentralized games and centralized games, and organized the Shell Chain team to solve various problems in the game field.

Terry

COO

As a consultant to the Aeria Games North America Operations Department, Aeria Games has achieved an average annual growth rate of 43% in North America for five consecutive years by providing reasonable marketing and advertising strategies.

Charles

CTO

A computer expert who specializes in telecommunications at the New York University School of Engineering and has a master's degree in computer science from Columbia University in New York. He has published 6 computer papers and holds 3 patents.In 2015, he worked as a technical consultant for Amazon Thailand in Thailand, focusing on the block chain and video game direction.

Patricia

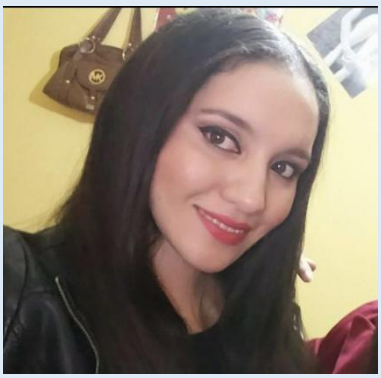
CMO

Sensitive to the game market, the free-to-play game model pioneered and personally promoted by Patricia dominates the game market today with more than 600,000 fans in the gaming arena.

George

block chain engineer

Senior block chain engineer, who touched bitcoin and block chain in 2011, has studied eth and eos public chain technology in depth, has a deep understanding of the public chain, has rich experience in public chain development, and has repeatedly built new startups from scratch. A decentralized application that can develop and maintain multiple different applications.



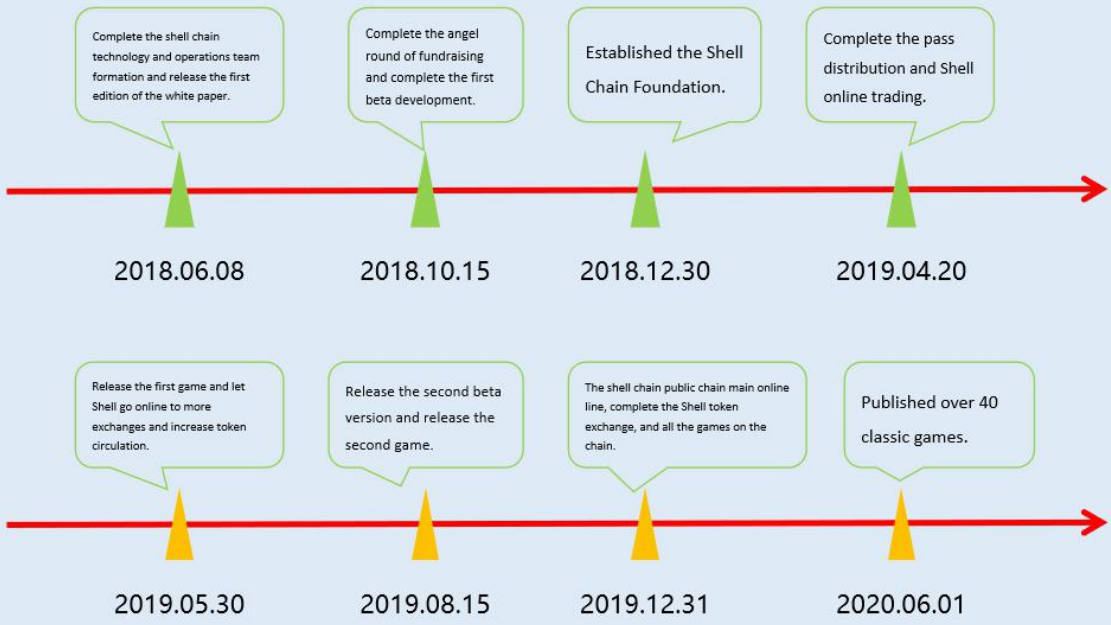
Jessica

Product manager

Senior visual engineer and commercial software consultant and product director specializing in product development and product architecture.

七、Cooperative institution

八、Development roadmap



九、Disclaimer and risk warning

This document is for informational purposes only and does not constitute an opinion of the purchase or sale of the Shell.Any similar offer or levy will be made under a trusted clause and with the applicable securities laws and other relevant laws, and the above information or analysis does not constitute investment

decisions or specific recommendations.This document does not constitute any investment advice, investment intention or instructed investment in the form of securities.This document is not intended to be an understanding or offer of any purchase or sale, or any invitation to buy or sell any form of securities, nor is it a contract or commitment of any kind.

We do not make any form of commitment, nor guarantee the intrinsic value and appreciation space of Shell tokens. Mining needs to fully consider the token price risk factor, and avoid using funds that exceed their own losses to participate in the game.

Participation in the game may face losses, players must bear any risk they face, the shell chain project team only serves as the technical support team of the project, and is not responsible for the problems caused by non-subjective game project operations, to ensure that the book is carefully read before the game. White papers and full understanding, please participate in this project carefully, if you can not bear the corresponding risks, please do not participate.

Countries around the world have different laws and regulations on cryptocurrency, block chain and DApp. Players need to fully consider the laws and regulations of their countries and regions, and ensure the legality of transactions and game behavior. The shell chain team does not induce any player to violate the rules. Any place, the intent of national laws and regulations.