NIRVANA

BLOCKCHAIN

PUBLIC CHAIN

Resources
NA Berry OS

The Turing complete programming language N++
Virtual machines and smart contracts
N++ IDE Visual programming environment

NA PC
loop signature
Antiquantum computing

NA WHITEPAPER 2.1.1

Cross-chain operation
NA Software Development Kit
Consensus mechanism
Distributed storage
Privacy Protection

Abstract

In the 21st century, mankind has entered the digital circuit age from the artificial circuit age. Human information system has also entered a centralized distributed system from the original stand-alone system, and today human beings will embark on a new journey in history: decentralized distributed information system.It is well known that in a distributed system with many nodes, each node is characterized by a high degree of autonomy. Nodes can be freely connected to each other to form a new connection unit. Any node may become the phased hub, but it does not have the mandatory hub control function.The influence between nodes will form nonlinear causality through the network. This kind of open, flat, equal system phenomenon or structure, we call it decentralization.

With the deepening of the interaction between subject and object and the constant balance between cognition and function. With the continuous improvement of cognitive structure, individuals can get rid of the egocentric state, which is called decentralization.Decentralization is not about not having the hub, but about choosing the hub by the node and deciding the hub freely. To put it simply, centralization means that the hub determines the node. The node must depend on the hub, nodes cannot survive without the hub. In a decentralized system, anyone is a node and anyone can be a hub. No hub is permanent, but phased, and no hub is mandatory to the node.

There are a lot of mature decentralization solutions out there, but they're not good enough. As a result, their practical application is very weak, not enough to be used for commercial use, or even to solve the development of traditional applications. Based on the current pain points, Nirvana（NA）puts forward a new concept of technology platform, and successfully constructs an ecological solution for the construction of IT information system （Network Omnipotence Application）that can be quickly implemented.

In the process of the continuous development of the blockchain industry, disorder is the biggest incentive to cheat. Centralization and low level of decentralization are the key resistance to impede the development of blockchain technology.In a disorderly market, the industry needs some advanced forces to make structural changes.

Abstract

We hope in the upcoming and further projects in the future, there will be no centralized authority phenomenon, a wide range of NA community members to guide the project development direction, rather than a single core team to decide the future of the project, the NA of the future will be also should be more team maintenance, more community consensus, 100% belong to all NA holders, truly make NA community consensus become robust basis, rather than an elite group of exclusive.

NA is born for application, it is to handle the whole network application infrastructure, as well as achievements in new blocks of chain management pattern. While building consensus for itself, it will provide benchmarking cases for the industry as a leader. As the outstanding advantage of NA, the output of values and ideas will be of better reference with the gradual improvement of the governance framework.

High quality theories and numerous and scalable applications will jointly contribute to the future ecology of NA and become a solid force leading the industry.

Whether you recognize it today or not, we are quietly changing the future of the world! The new informationization journey of mankind is coming again! NA public chain for the application of life, change you, change the world, change the future!

Nirvana Chain

5 Ecological roadmap

Public chain carry forward plan

Stage of ecological development

6 Team information

Jonathan Lancaster

Berton Carter

Craig Thompson

Milmar Ramirez

7 Risk warning

Insufficient information

Risks associated with judicial supervision

cryptography

Development fails or is abandoned

Source code defects

Source code upgrade

competition

Token Liquidity and Price Volatility

Accident risk

Reference：

Reid, Alex (1995). "IT Strategy Review, Distributed Computing — Rough Draft". Retrieved 2013-11-06.
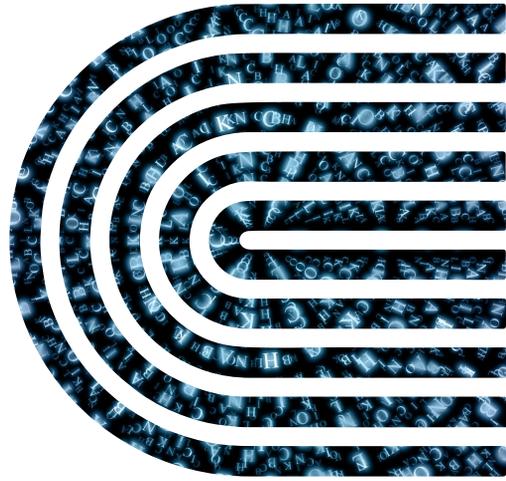
Nirvana Chain

1
Background and Vision

A common chain is the infrastructure of a decentralized information system

The drawback of traditional public chain

Traditional smart contract issues

NA vision

A common chain is the infrastructure of a decentralized information system

All decentralized applications need to be built on corresponding ecosystem, just like a website needs to run in a Web container. The platforms that dominated the interactive Web era in the past are: ASP, ASP.NET, PHP, JSP and so on. These development languages have enabled the Web to enter an era of rapid development. The best way to build a decentralized application is to develop the application on a platform with its own decentralized characteristics, and NA Chain is a decentralized infrastructure that has been heavily optimized and customized for application development.

The drawback of traditional public chain

There are many problems with traditional public chains. Let's list them and explain how we solve these problems.

01 Developer Issues

02 Security issues

03 Operation efficiency

04 Regulatory issues

05 High cost of learning

06 Traditional smart contract issues
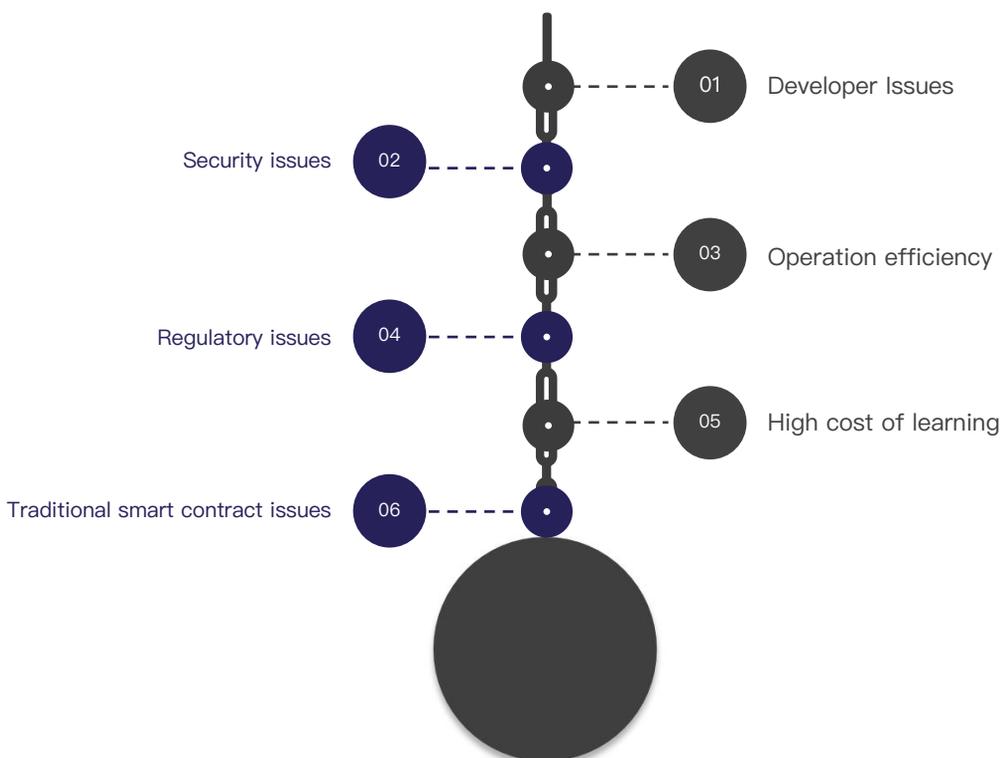
The drawback of traditional public chain

Developer Issues

• High cost of learning

At present, the learning threshold of all public chain application development is relatively high, and many traditional technicians are difficult to transfer from the original development to blockchain application development. Web services technicians are by far the largest group of developers in the world. These technicians had to relearn a new programming language, such as Solidity (ETH), WebAssembly based on C/C++ (EOS).In our tests, if a technology requires technicians to relearn new grammar, most technicians will wait and see. Unless he or she is currently working on a project that requires the technology, he or she will try to address the development needs with his or her existing technical knowledge. NA public chain for Web technical personnel technology low threshold to start the characteristics of the development of an epoch-making new programming language: N++ (N Plus Plus), by N++ programmer can easily realize their own interactive system development, especially based on the Web application system. If you already know a web-side programming language like ASP/PHP/JSP, we're pretty sure you can learn it in 5 minutes.

Command	Code Demo
Get the username variable from the form and store it into the username variable automatically	#request("username");
Get the username variable from the form and store it into the variable uname automatically	#request("username","uname");
Output variables to a Web page	<html><body>User:$uname</body></html>
Save the data to the specified DAPP blockchain	Blockchain.open("dapp address").insertDAG("Hello world!", "sign data");

Does the above code syntax sound familiar? Yes, all command syntax is that simple. Emphasize again, if you are a Web programmer, congratulations, in 5 minutes you can learn how to use NA Chain to develop a decentralized application/website/contract of your own...

- No good development integration environment

As an efficient programmer, we will have the corresponding development tools when we develop in the corresponding programming language:

programming language	Develop IDE tools	evaluation
C++	Microsoft Visual C++	A●
C#	Microsoft Visual Studio	A●
Java	IntelliJ IDEA/Eclipse	A●
PHP	Zendstudio/phpStorm	A●
Solidity (ETH)	Remix IDE(web)/ other IDE plug-in mode integration, can not release the application with one click	B●
WebAssembly(EOS)	Other IDE integration, not official website, output via C/C++/Rust	C●
N++	N++ IDE integrated development environment; One-click publishing applied to the public chain; Quickly create contract templates	A+●

A+●　　A●　　B●　　C●

Easy to learn

Fit

Development difficulty

Scalability
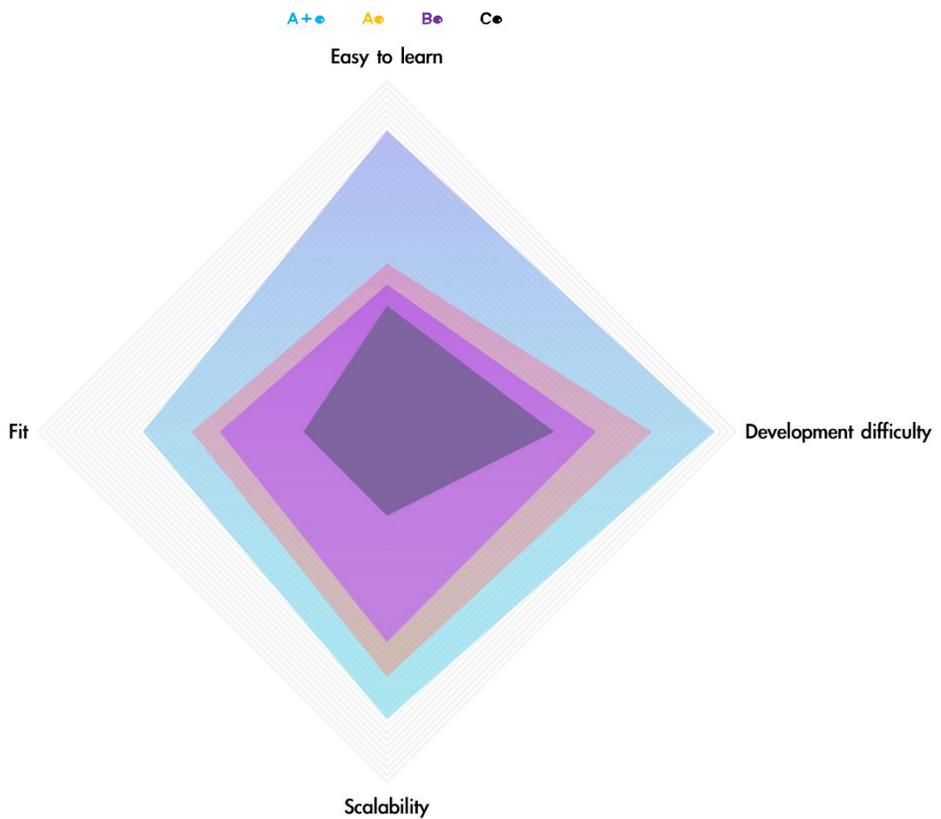
The drawback of traditional public chain

Operation efficiency

The current performance problems of the public chain focus on verifying the performance of the data stored on the disk. The main reason for the poor performance of this problem is the consensus algorithm. All consensus algorithms have their advantages and disadvantages, and often the public chain only rigidly provides a consensus algorithm to use, so that you're limited in developing applications by the consensus features. If the public chain is based on the consensus made by PoWF, then the dapp you develop can only achieve the performance of the consensus made by PoWF. If the public chain uses the POS consensus, then your application performance can only be limited to the performance of POS. In order to solve this problem, NA (Nirvana) Chain adopts the heterogeneous composite Chain pattern, which releases all applications independently on a dedicated instance Chain, that is, each application has its own composite Chain. Instance chain is composed of logical chain and data chain. The logical chain is mainly responsible for the maintenance of consensus, while the data chain is mainly responsible for the storage of a large amount of data. Through such a framework, the public chain achieves the effect of divide and conquer, and obtains the high performance of massive concurrency at the same time. Because N++ provides the function of asynchronous micro–service, a large application can be split into dozens of small instance chains, thus achieving million–level TPS. The current default instance chain consensus algorithm is: DPoS +DAG. In the future, we will continue to upgrade more consensus algorithm combinations, so that the instance chain has the hot–pluggable infinite expansibility.

Cost

• High transaction fees

BTC's annual gas bill is about $30 million, ETH's annual gas bill is about $20 million. However, BTC consumes $2 billion of electricity a year, and ETH consumes $430m. It is not difficult to see that the gas charge can only cover part of the electricity bill, and cannot cover the input and output costs at all. Judging from the development of various mainstream public chains, transaction costs of blockchain systems have been falling. However, the hardware and software costs of distributed bookkeeping are higher than those of centralized bookkeeping, but they must be much lower than the total cost of centralized bookkeeping. Through relative centralization, the transaction costs of chains have been greatly reduced. In order to pay for the high transaction costs, the blockchain industry has been looking for high–margin industries and and larger commercial cooperation to reducing transaction fees. The key is to reduce the operation cost of the machine. NA greatly reduces the cost of data storage through the hybrid consensus model. For example, use data stored by DAG, we can reduce the handling fee to a very low level.

The drawback of traditional public chain

•   High cost of operation and maintenance

In the case of IPFS, the current consensus hardware input cost for IPFS is several times that of traditional storage solutions. With this feature, the cost of storage is difficult to reduce, unless the Internet data duplication, after a large number of platforms are connected to IPFS, its cost is likely to be reduced. However, this is something that traditional CDN caching technologies already do. And now all Internet platforms do the deep ploughing subdivided vertical fields, so that the data on their platform is unique. There will be no duplicate data throughout the network. Even video sites, their data is also watermarked. Imagine a video watermarked on YouTube. Do you want to appear on another video site? The answer is definitely not, every platform wants its own video exclusive, brand personalized. This makes it difficult to reuse a single piece of data across multiple platforms. Some high-reuse files may eventually be separated by system integration or CDN caching technology. Using existing resources is the most cost-effective, today if the public chain for the public chain to purchase some of the latest hardware servers, then your cost will never come down. NA public chain supports the access of all traditional Web servers, so that all servers can access the public chain network to provide services, thus reducing the operating cost.

Security issues

•   Some data is exposed indefinitely, lack of privacy.

Data privacy is an individual right, and at the same time it is the bottom line for individuals and organizations, as well as certain industries involving a large number of trade secrets and interests. Building a robust system of trust is also the vision and expectation that blockchain attracts many adherents. On the surface, blockchain technology seems like the perfect solution to this problem, since blockchain transactions don't need to be tied to identity information, and anyone in the world can create an anonymous wallet and conduct transactions. The problem is that we use a common, easily traceable ledger. Trading records, and stored in books in the public, and with only consists of numbers and letters associated account address, because there is no binding the user's real information, thus produce misleading, unable to track entity and ensure privacy for the individual, it ignore the current public chain of data transmission and storage is publicly observed facts, such as intelligent all the details of the contract, including the sender, receiver, transaction data, execute code and storage conditions.In fact, this "pseudo anonymity" that guarantees privacy is the last layer of secrecy that impedes privacy. Once someone finds the connection, all privacy disappears. This also breaks the premise that blockchain transactions are completely anonymous.

The drawback of traditional public chain

• If the number of data nodes is too small, it is vulnerable to dust attacks.

The first criterion for a public chain is the number of nodes. The international technical standard is that a thousand scattered nodes that cannot be controlled at the same time can be called a public chain. This is one of the reasons why Bitcoin and Ethereum have been embraced by the industry. The heart of decentralization is the node mechanism. A truly distributed compute node must have enough nodes to participate, because a sufficient number of nodes represents reputation, and cannot be tampered with to achieve sufficient decentralization to prevent malicious attacks between nodes, such as dust attacks, etc. Therefore, the entry and exit of nodes should be free to enter and exit according to the rules, and the threshold of nodes should be low enough to allow more data nodes to participate. The active participation of community members is also the core spirit of blockchain. In order to achieve the addition of more nodes, NA adopts the mode that full nodes can maintain all instance chains, which greatly increases the number of full nodes.

• Higher security

In the traditional public chain design, the computation and storage of the computing layer are not separated. Most public chains use GAS mechanisms to balance the computing PoWFer of the main network. There are actually two problems with this design. First, the computing resources of the main network are not separated. As a result, uneven distribution of computing PoWFer can lead to network congestion, and cannot even execute a DAPP with less computing PoWFer. Second, there is no separation between contract behavior and transaction behavior, thus creating the possibility of wallet theft. The system security of the public chain needs to be improved all the time, including attacks from external entities (denial of service attacks, DDoS, etc.), attacks from internal actors (mock attacks, witch attacks, Collusion attacks, etc.). Fault and computing PoWFer attacks, double-flower attacks, transaction and contract vulnerability defense mechanisms, identity and anonymity, database security, etc., and even combat quantum computing to address all kinds of privacy leaks, fraud, and transfers. The public chain in the era of digital economy will face more users, it must meet higher standards in security audit, security architecture, compiler security optimization, virtual machine security design, contract security template and other aspects, in order to meet the security needs of users.

The drawback of traditional public chain

Regulatory issues

•   Anyone can participate anonymously, lack of appropriate monitoring strategies.

The centralization of blockchain makes many public chains or projects inevitably in the opposite direction of centralization, which is actually the mode of operation of the main body in today's society. The mode that everyone can participate anonymously also encourages insecurity to some extent. The ultimate use of blockchain technology must be to solve social problems and increase productivity. In order to realize the popularization of commercial applications and the promotion of social value, the architecture design of public chain must consider how to solve the conflicts and frictions with the traditional central regulatory authorities and how to integrate with the central society in the real world. So far, in the traditional public chain research and development field, and even the whole blockchain industry, there is no safe way to upgrade, and there is also a lack of legal provisions and reference standards to formulate methods and maintain regulatory provisions. More developers, professional legal practitioners and other relevant personnel are still needed to support and participate. The exact implementation is not yet clear, as it is difficult not to have an environmental mandate in the standards center, but the regulation has begun to actively touch on all areas, and will become more stringent, in this situation, will be more secure against new issues and challenges in the industry.

•   The reward system is chaotic and manipulable

Incentives are known as the core driving force of blockchain. The aim is to integrate the value of all stakeholders in the system as an incentive for participating nodes to participate in block validation. A robust reward system like Bitcoin should be able to satisfy the incentive feedback quickly and continuously, without ending for any reason, and always maintain positive incentives so that full nodes can spontaneously keep the whole system running in a healthy and orderly way. The incentive mechanism of the public chain network system provides a new idea for many developers, and produces many different incentive mechanisms. In order to get more nodes to participate, many mechanisms violate the original intention of incentives and take the right to reward in their own hands, rather than putting the maintenance of the whole chain in the first place, which makes the market full of chaos.

The drawback of traditional public chain

Scalability issues

The architecture of digital assets is unsuitable for DAPP in many ways, mainly in two aspects:

• Not easy to use

Blockchain technology integrates many technologies in computing, networking, encryption and other fields. These techniques are very specialized to the average user, such as private keys, public keys, addresses, encryption algorithms, consensus mechanisms, public chains, and other terms, enough to make the average user retreat. Even if users are willing to learn, they must go through many tedious steps before they can actually use the application. For example, if a user wants to use a smart contract–based DAPP, he/she must first do several things: First, he/she should get the wallet address and private key, and know how to use the wallet address and properly save the private key. Second, he/she must somehow get the ETH before he/she can transfer it to the DAPP's wallet address. For blockchains, this process is complex and usually requires a long wait time (more than a week) for a user to actually use the DAPP. Blockchain based DAPP should be used in the same way as traditional apps. A traditional App can be downloaded from the App Store and used for free or at a very low price. It can be seen that the traditional public chain cannot synchronize quickly because it cannot divide and rule the data. Therefore, for each new user, the first data synchronization of the wallet has become an obstacle.

• Single Application Scenario

All DAPP applications on a digital asset can only share one main chain. DAPP cannot build their own subchains, customize their own consensus algorithms, or choose the best configuration for business needs. As a result, digital assets are currently being released with few business application scenarios to support, which is not conducive to building the DAPP ecosystem. NA Chain can build different consensus algorithms for different application instances, and the data of DAPP can be divided and rule.

Traditional smart contract issues

In addition to the inherent drawbacks of traditional chains, there are many problems with traditional smart contracts. A smart contract is a computer protocol designed to digitally facilitate, verify or enhance the negotiation or fulfillment of a contract and allow trusted transactions to be executed without the need for a third party.

Traditional smart contracts have the following problems:

•   Contract issues

The scenario for a digital currency transaction is too simple based on the enforcement rules, resulting in extremely simple enforcement rules, which still fall far short of contracts in our real life. In real business and life, we need more and better contract rules and systems, especially for the financial sector, the complexity side represents security and flexibility.

•   Input credibility issues

There is no complete Turing contract, and parameter input is manual. Manual typing carries the risk of typing errors. It is important to support reliable data imports. When publishing an application, it is important to publish both the default data and initialize the data. Through the initial application release data initialization, it can reduce the handling fee generated by a large number of data entry transactions, and can realize the streamlined data import.

•   Execution issues

Timed tasks are not supported. Therefore, all smart contract triggers need to be executed by human execution of the request. But often in application development, we want to perform tasks at every block height. For example, report data generation and K line time–sharing line data are performed once a day. These requirements cannot be realized in the current smart contract. However, NA introduces timed tasks, where users can pay a prepaid fee to a smart contract to perform the corresponding tasks at a fixed time.

NA Vision

NA Public Chain hopes to improve the public chain ecology through its own advanced technology concept. Realize decentralized applications with low learning threshold and ease of use. The perfect application of the traditional technology ecology into the chain change.

NIRVANA
CHAIN

Illustration by digital artist Tiona Lugia for NA (Nirvana) Chain
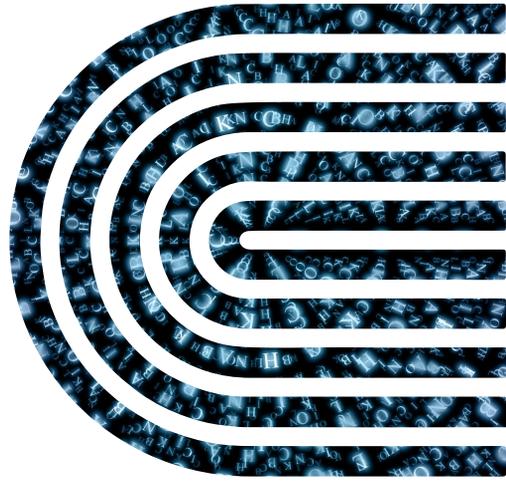
Nirvana Chain

2

Technical scheme

Infrastructure

Name	Paraphrase
Node layer	NA Chain nodes are divided into full nodes and ordinary nodes. After becoming a full node, all data of the whole network will be maintained. Normal nodes can choose to maintain the entire network data, or they can choose to maintain only a specific application instance.
Consensus Layer	The consensus layer is the core part of the blockchain protocol, defining the consensus algorithm and the block data paradigm. NA uses an innovative heterogeneous complex chain consensus mechanism, and users can choose the consensus mechanism most suitable for their application needs.
Instance layer	All applications are instantiated into a composite chain that provides business support for the application.
Application layer	Based on NVM virtual machine, the application by the virtual machine to perform logical operations.

Design goals

NA is designed as an application-oriented public chain that supports multiple consensus mechanisms, distributed storage, dynamic pricing, anti-quantum computing, cross-chain operations, and other innovative technologies, as shown below:

PoWF+DPoS+DAG Consensus Mechanism

Name	Paraphrase
Application main chain	Based on PoWF consensus mechanism
Application example	Instance logic chain(DPoS/user-designed)+Instance data chain(DAG)

Design goals

Application main chain （PoWF）：

All applications need to be registered or uninstalled on the main chain when they are released.

Application full nodes（21 * N）（DPoS+DAG）：

To gain the right to account, all the nodes need to vote for the super node using the NAC. The relevant NAC will enter a 3-day lockup period. After the lockup period, the votes can be cancelled and re-cast. To deposit is to vote, and to withdraw is to cancel, so the votes of each candidate node will change for each round. A block is generated every 6 seconds, and each supernode can get 10 block rights. Total: 21 nodes *N*10 blocks =210 block cycles, equivalent to 1260 seconds to complete one round. After voting, the corresponding supernode will get the block right. If, during the block drawing process, a supernode cannot work normally, as long as more than 70% of the nodes vote to determine that a node is not working normally at this time, the remaining blocks will be completed by the previous node. The corresponding node device needs to be online when voting, because the device responsible for checking the ticket will attempt to connect to the IP address and will skip the node if the connection is not possible. The voting system elects early the next batch of names, for example, if you are currently at the height of Block 1, votes will be selected from the height of Block 211, votes from the height of Block 421 will be selected, and so on.

Income earning conditions:

• Holds Full Node Credentials in Full Node Credentials application; After obtaining the credentials, you can download random questions for performance testing. Scores for each round of testing are automatically linked. Used to highlight the computing performance of the device.

• Have a separate public network IP address;

• The inspectors will try to connect to voters' addresses to check the network status, thus forcing all miners to have equipment and be online. If it is not found online, the node is automatically skipped.

Design goals

Income allocation scheme

The proportion	Beneficiaries
3%	21 supernodes
77%	Make full node voting device that casts 21 super nodes
10%	All full node devices participating in the voting
10%	All devices participating in the voting (full node + normal node)

- Supernodes get 3% revenue

- Full-node voting devices holding NAC receive 77% of the revenue weighted equally by the number of votes cast, and full-node candidates receive 10%.

- The remaining 10% will be weighted equally according to the number of votes (ordinary sections + full nodes can also participate), with 1 vote for each NAC and 100 votes for the initial limit of each device. Voting equipment needs to be kept online.

Design goals

Apply Common Nodes（DPoS+DAG）

Normal nodes can be specified to maintain only one or more applications, earning a bonus for a specified application block. Maintaining a specific application also requires voting using NAC in the application's voting system. The 21 super nodes in the default full node are the default work nodes for all applications. If a new voting node appears, it replaces the default node. Normal nodes can also participate in the application mainchain consensus, but only receive 10% of the net voting device weighted share revenue, and the other 90% will automatically enter the destruction pool until the destruction stops.

Income earning conditions：

- Normal nodes can vote NA full nodes. Obtain 10% of the weighted profit of the whole network voting equipment, and cap 100 votes per device.

- Nodes need to stay online after voting. Otherwise, they will be excluded. Data applications also need to be available, because the inspector will make access requests along with the machine request node to ensure that the published application service is available.

Apply Full Nodes	Apply Common Nodes
–AFN–	–ACN–
Income earning 100%	Income earning 10%
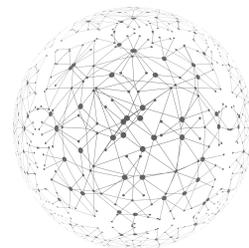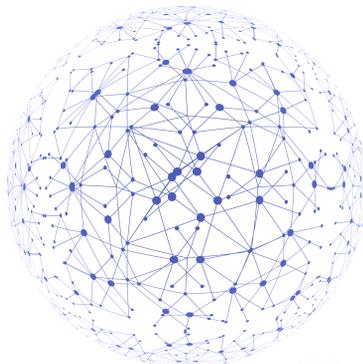
Design goals

Resources

Name	Description
Ordinary transfer GAS charges	Constant 0.01 USDN
Complex computing GAS charges	Perform complex computation, calculate the computation amount by NVM, and charge the corresponding Gas fee.
Store Gas	All nodes can set the lowest price in the certificate, and the average price will be updated every 14400 block in the certificate application. When the application is packaged, the price cannot be lower than this price. Full-Node Miners set the price per app at 100USDN when the app is released.

The average price algorithm = the voting prices of all nodes are sorted, and the middle 51% data is taken for average calculation.That is, after removing the top and bottom data of the olive type, the mean value is calculated. That is,the data obtained after removing 24.5% from the top and bottom respectively.

Distributed Storage

NA-Distributed File System is a group of Distributed storage protocols using Distributed hash table technology. DFS indexes data by the content of the file (hash) rather than the path to the file (URI). Large files are divided into fixed-size blocks of data that are distributed across multiple nodes. The main problem with such a system is to strike a balance between redundancy and reliability. DFS plans to solve this contradiction through token incentive mechanism and the establishment of backbone nodes. The user can choose the reliability requirements of the file. The files with low reliability can be stored and accessed for free or almost free. The backbone node (full node) will provide high reliability file storage for the stable and reliable files.DFS will set access rights for these files through the contract. In addition, DFS can be used in conjunction with digital identities to issue, transmit, and revoke digital certificates that record digital identities point-to-point, without having to be managed by a centralized server. In the future, old blocks of data can be stored in the DFS so that most full nodes can release the old data, achieve greater scalability, and ensure the integrity of historical data. The storage price is set by the device owner, and the cost will be paid to the device owner in a step-by-step manner.

Design goals

Antiquantum Computing

In the current blockchain system represented by Bitcoin, SHA-256 hash computation and ECDSA elliptic curve cryptography constitute the most basic security guarantee of the Bitcoin system. But with the continuous breakthrough of quantum computer technology, especially the quantum algorithm represented by Shaw algorithm can theoretically realize the transformation from exponential to polynomial level.

These "hard" problems of the classical computer will be solved by practical quantum computers in the foreseeable future. Most of the existing blockchain systems use ECDSA, but SHOR attack algorithm is very effective for quantum computer ECDSA signature algorithm, SHOR algorithm is suitable for solving large integer decomposition, discrete logarithmic inversion and other difficult mathematical problems, resulting in ECDSA signature algorithm is very insecure. Considering the high security of digital currency transactions under the quantum attack, NA adopted the lattice theory based signature algorithm NTruSign -251.

Cross-chain Operation

NA adopts the heterogeneous cross-chain solution of blockchain, and re-implements the instance chain of the corresponding target public chain data structure in NA, and synchronously maintains the data of this chain. The data source is provided by 21 nodes that are secure and reliable.

For example, if we need to interconnect with Bitcoin, then we can produce a chain of Bitcoin instances. All data is synchronized with the data of the original Bitcoin public chain. All transport protocols adopt the design of the original chain to realize the interconnection between independent blockchains and ensure the effectiveness of cross-chain transactions and the security of users' private data. Through this design, it can ensure that the functions of the original target chain can be realized in the original public chain, without too many additional technical obstacles.

Design goals

Privacy Protection (ZK-SNARK Zero-Knowledge Proof Algorithm)

ZK-SNARK zero knowledge proof algorithm is one of the more mature and feasible privacy protection technologies, with better anonymity. It does not require trusting the participation of the central node or other users in the network. Users can realize anonymous transactions by interacting with anonymous currency, thus effectively protecting users' privacy.

As the carrier of forwarding and verifying cross-chain anonymous transactions, it needs to be able to verify the effectiveness of cross-chain anonymous transactions. Cross-chain transactions can be divided into two categories: cross-chain transparent transactions and cross-chain anonymous transactions. Cross-chain transparent transactions provide the content of the transaction itself and the associated Merkle branch evidence. The verification nodes in the interconnected chain network can verify the validity of the transaction according to the verification rules of the parallel blockchain registration. Anonymous cross-chain transactions do not disclose any information except the validity of the transaction.

Validation nodes in the Internet network need to be aware of the public parameters generated during the start-up phase of each parallel blockchain network and use these public parameters to verify the validity of anonymous cross-chain transactions. Blockchains and zero-knowledge proof algorithms ensure that no information other than the validity of cross-chain transactions is compromised by the verification nodes in the interconnect network.

zkSNARK
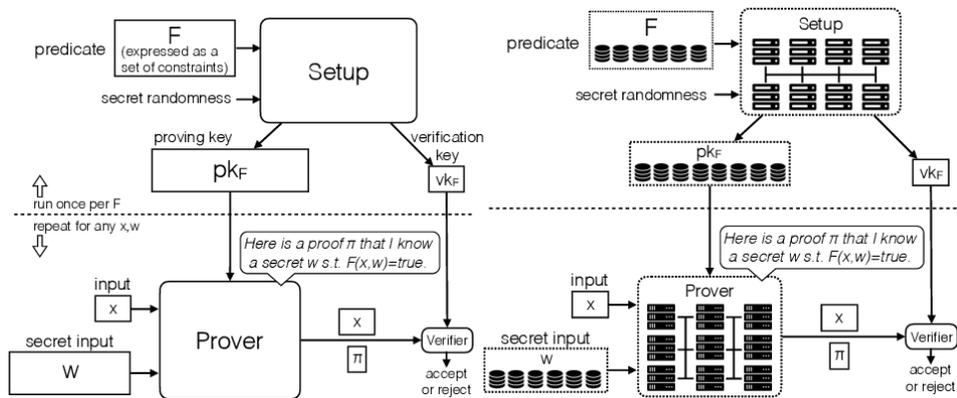
NA proposed a cross-chain transaction privacy protection method based on ZKSNARK algorithm

Design goals

Loop Signature

NA implements the anonymity of digital assets through loop signature technology. The loop signature technique is described as follows:

A public signature, with only one participant, is shown below, which can be mapped one-to-one. A loop signature obscures identity because it is just someone who belongs to a group without knowing who is in that group.

This allows for a high degree of anonymity in virtual currency transactions, which can be seen as a combination of decentralization and distrust. In order to remain anonymous, NA uses a one-time loop signature technique. Loop signing works by allowing the initiator of a transaction to join the group and then to join the transaction as a unit, rather than allocating privacy from a single private key signature. This technique allows the initiator to mix. The verifier can prove that the output exists and that one of the members of the group is a true signer. However, because each member has an equal probability weight, they cannot determine which group member the signer is. As the group size increases, the likelihood that each member will be a true signer decreases. Loop signatures, which involve merging the user's real hidden address P, and a large number of "virtual" P scattered across the blockchain. The signature is verified by all P's, and mathematically any corresponding private key can sign the transaction, thus obfuscating the identity of the real sender. To prevent double spending (which means that the same money appears in two or more transactions at the same time), each NA transaction has a unique key image. The key image is created by taking the hash of the hidden address P and multiplying it by the private key, which is different for each transaction. This mechanism ensures that each P can be used only once. The NA network maintains a database of all incomplete key images, so if a user tries to reuse a key, the network will reject the transaction.

Design goals

Virtual machines and smart contracts

• NA Virtual machines

NA Virtual Machine is a lightweight Turing-complete Virtual Machine developed for the NA ecosystem. It is a high-performance blockchain network distributor designed to provide efficient, convenient, stable, secure and scalable custom blockchain systems. The virtual machine concept explained in this white paper is very narrow. It is not a simulation of a physical machine through an operating system. NVM supports micro-service architecture, and has dynamic parsing function, which can realize dynamic rendering development of Web (similar to ASP/PHP/JSP). The complete operation process is as follows:

Step	Paraphrase
01	Compile smart contract source code to bytecode.
02	Push the bytecode and associated parameters into the execution heap as the run context.
03	Whenever the execution engine retrieves an instruction from the current context, it executes the instruction and stores the data in the computation stack and temporary stack of the current context.
04	If external data needs to be accessed, it will use an interoperable service.
05	After all scripts are executed, the results are saved in the results stack.

Design goals

NA super smart contract

The programs released by NA are all decentralized programs. The suffix of the filename is ".na ". For example, when the user logs in to userlogin. na, this is the source file, and the compiled file is uselogin. nac, or userinfo. NSP if you want to publish dynamic web pages.

File type	Suffix type	Similar to the
N++ program source file	.na	.java、.cs
N++ program binaries file	.nac	.class、.exe
N++ dynamic web pages	.nsp	aspx、php、jsp

	Step	Paraphrase
common smart contracts	01	NRC Token Contract
	02	Asset custody requires multiple people to sign a contract, and digital assets transfer requires multiple people to agree
	03	The custody of senior assets requires more than one person to sign the contract. If all the members agree when transferring the currency, it will be successful immediately. More than 67% of voters agreed, and no one voted against it in three days. More than 33% of the voters agree, 90 days no vote against, the successful withdrawal of the currency; More than 10% of the voters agree, and no one votes against the proposal in 180 days.
	04	Trust contract: suitable for trust financial management, such as the living expenses for the son, which will automatically release 3000U every month. The son needs to come to collect by hand every month.
Super smart contract	01	Can develop complex computing systems, such as OA, ERP, e-commerce, data analysis, big data, industry systems, etc.
	02	Can dispatch nodes to carry out complex operations, improve the calculation speed. Each dispatch a node need consumes Gas.
	03	Parallel computing, AI, image recognition, large-scale complex operations, etc., can be realized by dispatch GPU chips.
	04	Special components: video push and pull stream, picture storage.

Design goals

The Turing complete programming language

- syntax introduction

commands	syntax
comment	Single–line comments ## This is a single line comment. Multiline comment #* This is a one line comment. This is a two line comment. This is a three line comment. *#
variable	Setting of variables： #var($age= "28") The name of a variable can be composed of the following characters: alphabetic (a .. z, A .. Z) numeric (0 .. 9) underscore ("_") Variable references: Variables are referenced using the leading $, dollar sign $user $sex $age
Obtain data	request instance： https://domain.com/login?Username=david&age=25 Store the obtained value in the variable named uname #request（"username", "uname"） The obtained value is automatically stored in a variable named age #request（"age"）
method	$user.getAge() $page.getTotal() $page.setTitle("My Home Page")

Design goals

Conditional instruction	All instructions are preceded by # sign, which needs to be preceded by # sign as a declaration.
	Conditional statement
	
	Example 1:
	#if($user.getSex()==1)boy#{else}girl#end
	
	example2：
	#if($show)
	  NA Server Page!
	#end
	
	example3：
	#if($age< 10)
	   School
	#elseif($age== 18)
	   Liquor
	#elseif($age== 28)
	   Married
	#else
	   Nothing
	#end

LOOP instruction	 #foreach($product in $allProducts) $product #end
dynamic reference	Refer to other code in the application and execute it in combination #import("tokenUtil.nac") This contract refers to the code in another contract: #import("dapp address", "tokenUtil.nac")
Static reference	Loads the data of the specified file and makes an assignment #include("kline-20190101.txt", $klineData)
Save to the blockchain	Open the specified dapp application: #Blockchain.open("dapp address", $dapp1) Save the data: # Sign the data with my private key and save it to the data chain. # InsertData and insertDag have the same effect $dapp1.insertDAG("Hello world!","sign data"); # insertLogic and insertDPoShave the same effect $dapp1.insertLogic("Hello world!","sign data"); can also use a one-line instruction #Blockchain.open("dapp address").insertDAG("Hello world!", "sign data");
Dispatch contract method	Open the specified dapp application: #Blockchain.open("dapp address", $dapp1) $dapp1.call("evenName", $callbackData)

Design goals

- establish application

Application Type	Paraphrase
smart contract	You can easily select the corresponding contract template for contract creation in the IDE, or you can create your own template. All contract templates can be used on their own, or they can be published to others to become contract standards for more people to use. Once the contract is written successfully, it can be submitted to the test chain for testing. After the test is passed, it can be submitted to the main chain.
Create DAPP	Creating DAPP is like creating a contract. You create your own application system in the IDE, and then write the corresponding business logic code. At the same time, it can also make a Web–based UI interface for data interaction. Of course, the UI part can also be displayed by desktop software or mobile software. This depends on the needs of the user.
Create DWeb	To create the DWeb we will not only wrap up the logic part of the code, but also open up the interface part as well. In this way, the benefits of chaining on the interface can be easily realized. The application can be completely decentralized. After the successful launch of the website. You also need to register the site with the NA DNS system to get a dedicated access domain name.
Create desktop software	NA software development includes the Desktop SDK suite, which makes it easy to develop Desktop software applications with executable files. Details will be published on the official website later.
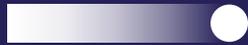
Design goals

- Application publishing/uninstalling

1) Publish the application to the public chain

You can use the tools provided by NA to install the application. It is also possible to install and distribute with a more user–friendly online application.The written project directory application is packaged by the console instruction. The packaging instruction is as follows:

Package	Nac.exe –packaging

Publish	Nac.exe –install –appname –version –type –owner –ownerSign

Parameters	type: standard（default) immortality（not uninstalled)

2) Release app to the NA Appstore

After the successful release of the application, users can submit their own software in the application market, upload screenshots, ICONS, descriptions and other information for the software.

3) Uninstall in the application chain

Uninstall the application using the tools provided by the NA official. It is also possible to uninstall using a more user–friendly online application.

Uninstall	Nac.exe –uninstall –appaddress –owner –ownerSign

Design goals

N++ IDE Visual programming environment

Through the development tool, we can write the.na program file to compile, at the same time can also be in the local simulation browse run. In order to achieve the local stand–alone environment and can also be software development, testing, browsing.

1) Compile the compiled.na file to.nac

Through GUI programming development environment for software development, compilation.

2) Packing dapp/dweb packages

Through the GUI programming development environment for software or website packaging, release and other work. So as to reduce the user's learning threshold.

NA SDK（NA Software Development Kit）

The NA SDK includes the Desktop Development Kit, which allows us to develop applications based on Windows, Mac, Linux and other desktop systems. All the data will work offline. When connected to the network. All the data will be automatically submitted online.

This great feature allows users to easily developed offline POS machine, even if the user mobile phone no network at that time, POS machine also have no network, as long as by phone NFC data signature, as long as both parties have one party on the Internet in the future, the data will be broadcast to block chain network, thus offline payment data field. At the same time, the user can also work or document entry in the environment without the network. When entering the network environment, the data can be automatically published online.

2.2.13 NA PC （Hardware）

• NOS–based personal computers

<Based on the request of the original team, this part is temporarily confidential and will be announced according to the progress of the project>

• Function is introduction

<Based on the request of the original team, this part is temporarily confidential and will be announced according to the progress of the project>

Design goals

NA Berry OS (NA Operating System, NOS, Code: Berry)

Blockchain operating system based on Linux kernel

The Berry OS kernel is based on Debian, which is a completely free operating system. Debian GNU/Linux is an operating system and free software distribution that is maintained and updated by a group of users who volunteer their time and effort. We customised Berry OS based on Debian and highly integrated NA Chain into the operating system. And perfectly dispatch the resources of the operating system to provide application support for the whole public chain ecology.

Feature	Description
• **Stability**	There are many cases where machines that have been running for years have not been restarted. Even when machines do restart, it's because of a PoWFer failure or a hardware upgrade. Compare that to other systems that crash multiple times a day.
• **Faster and easier memory management**	Other operating systems may be fast enough in one or two areas, but Debian, based on GNU/Linux or GNU/FreeBSD, has low hardware requirements and is smooth. Windows software running through the emulator under GNU/Linux is faster than running in its native environment.
• **More stable hardware drivers**	Most hardware drivers are written by GNU/Linux or GNU/FreeBSD users, not vendors. This may mean that there is some delay, as support for some hardware is a process. However, hardware can continue to be supported long after the manufacturer stops production or goes out of business. Experience has shown that open source drivers are often far better than closed ones.
• **Good system security**	Debian and the free software community pay great attention to fixing security issues quickly in software releases. It usually takes only a few days for a fixed piece of software to be uploaded. Because it is open source, Debian's security is evaluated when open. And other free software projects have the same level of assessment systems to prevent potential security issues from being introduced into the base system in a significant way.
• **Security software**	Many people don't know that any machine can see any information you send over the network. Debian has the famous GPG (and PGP) software that allows messages to be sent secretly between users. In addition, SSH allows you to create secure connections with other machines that have SSH installed.
Built-in application	• NA Browser • NA distributed disk management • NA application market • NA wallet • NA DNS • NA N++ IDE
Introduction to built-in commands	<The final command shall prevail after the project goes online>

Built-in application

NA Core tokens

- NOMC Voucher Token

Nomc Voucher Token	
Total	35,000
circulation	15,000
Final Retention (The autonomous community will vote on whether to open the unlocked parts)	20,000

Full node credentials	
Full node operation mode	Maintain all network data and consensus. Full-node mode is started in such a way that the mining miner's block chain address holds the full node certificate. Full Node Credentials can be exchanged in FNC DAPP.All nodes receive full block packaging benefits. ◆ Note: Please use the miner's address for the exchange.
Normal operation mode	Miners that do not enter full-node operation mode will be maintained in normal operation mode by default. The block package reward is only 10% of the weighted profit of the whole network voting equipment.

Built-in application

- NAC public chain tokens

NAC public chain tokens	
Total	75,000,000
Destroied	28,000,000
Final Retention	47,000,000
Application relevancy	• Create common application publishing fee, one-time destruction of 10% • InstallPack App is released in InstallPack mode with a one-time destruction of 10% • Transfer fee GAS, 10% for each transaction • NA AppStore releases to the App Market destroy 10% per year • NA DFS rental fee, 10% per order destroyed
Destruction mechanism	• NA DNS rental fee, 10% per annum destruction • NA FNC converts all node certificates, and destroys 100% at one time
Application Main Chain (PoWF)	All applications are instances, and each instance contains two chains. One for the logical chain, one for the data chain. The identity of the instance is written to the application mainchain.The main job of the application mainchain is to store the basic information of the application instances, which can be used to mark the availability of the application. Users can issue Install and Unstall directives to the application chain to request instantiated chain resources from the public chain system.
Application instance logic chain (DPoS)	All the business logic processing required by the application instances in the business interaction is completed by this chain. When the application is released, the application code file is packaged and compressed in a ZIP format. It is stored in the creation block of the logic chain. The maximum capacity of the creation block is 64M, so the compressed package cannot exceed 64M. Once the application is published, it cannot be modified. Therefore, it is important to ensure the reliability of your application when you release it. If the file size exceeds the upper limit, the resource files should be split up and stored in a cheaper static instance (NA DFS).
Instance data chain (DAG)	DPoS elects the DWorker work node. All DPoS recipients can receive the transaction data submitted from the external source, but only the DWorker work node can confirm the signature of the data. Other DPoS nodes are only collected as data and broadcast in the working cluster. Use DWorker mode to hide the real work node. Every 14400 block competes for a new DWorker node, which is once a day. All trades are completed in real time. Therefore, it is theoretically possible to achieve millions of concurrency on a single machine. Of course, this speed depends on the network environment and the miner's hardware performance. The selected work node can obtain the commission for all DAG transaction data. Ordinary transfer transaction fees are constant at 0.01 USDN.

Built-in application

Application Main Chain		
Release application		• After the application is released, the PoWF packaged miner will create the application instance chain, and broadcast all the full nodes for synchronization after completion. • After receiving the instruction, all nodes construct the data and chain, and maintain the data on the chain by voting. • After the successful creation of the application, can apply for an exclusive domain name in DNS. When the application is in the ready state, the DNS system is notified so that the DNS system can direct traffic to the node for service. • When an application is requested, it checks to see if there is an application in the cache, and if not, downloads the zip package from the chain and unzips it to disk. It is loaded into memory by NVM for execution and rendering.
Application of valuation	Pricing strategy	The average price algorithm = the voting prices of all nodes are sorted, and the middle 51% data is taken for average calculation. That is, after removing the top and bottom data of the olive type, the mean value is calculated. That is, 24.5 percent of the data is removed at the top and 24.5 percent at the bottom.
	Publish App Pricing	All nodes can set the lowest price in the certificate, and the average price will be updated every 14400 block in the certificate application. When the application is packaged, the price cannot be lower than this price. Full-Node Miners set the price per app at 100USDN when the app is released.
	Transaction fee pricing	All nodes can set the lowest commission price in the voucher, and the average price is updated every 14400 block in the voucher application. The transaction commission is constant at 0.01USDN.
	Contract dispatch pricing	Reading data is free, writing data is charged. The amount of computation to be performed, such as the computation calculated by NVM for complex technology and the corresponding Gas charge, 0.1USDN minimum.
Uninstall the application		Uninstall requires the author's private key to send the instruction. After uninstall, you will be rewarded with 5% of the cumulative transaction fee of this class.
Application commission	Miners earnings	85 per cent of the fees are miners' income, and 95 per cent after deflation has stopped.
	Destruction of deflation	10% handling fee enters the Destruction Deflation
	Uninstall the bonus	5% App Uninstall Bonus, which encourages app authors to uninstall apps that are no longer in use. After the application is uninstalled, the application will be automatically skipped if a new node is connected to the network for the first data synchronization. Thus save the system resources of the public chain. The app is also marked as unavailable and notified to the App Marketplace. The network will no longer synchronize related data and request access. The unload instruction specifies whether the application should jump to a new application. In order to be used as a new version of the software upgrade. The new app creation block has a default data function, which can be used to shift data from the old app into the new app. So that the old user's data can continue to be used in the new application. But this operation needs to be done by the software author himself.

Built-in application

		Application Main Chain
Coinage	Block production	60s/Block
	1 hour	60 Blocks
	1 day	1440 Blocks
	1 year	518,400 Blocks
	Initial coinage	1NAC/Block
Reduced production	Production reduction cycle	halving production every 4 years
	Final production per block	0.0625NAC/block (reducing production for the fifth consecutive time)
	Total period	107year
	Cumulative production in the tenth year	49%
	Final block height(PoWF)	55177296
Rules Block height	1 to 2073600	1NAC/Block
	2073601 to 4147200	0.5NAC/Block
	4147201 to 6220800	0.25NAC/Block
	6220801 to 8294400	0.125NAC/Block
	8294401 to 10368000	0.0625NAC/Block
	10368001 to 55177296	0.0625NAC/Block
Income	AFN	100%
	ACN	10%

Built-in application

Application instance logic chain		
Capacity limit	Creation block	64M
	Data block	8M
Transaction commission	Miners earnings	Eighty-five percent of the fees are the miner's income, and when deflation stops, it is 95 per cent.
	Destruction of deflation	10% handling fee enters the Destruction Deflation.
	Bonus of Uninstall	5% app uninstall bonus

Built-in application

Application instance logic chain		
Coinage	Block production	6s/Block
	1 hour	600 Blocks
	1 day	14400 Blocks
	1 year	5,184,000 Blocks
	Initial coinage	1NAC/Block
Reduced production	Production reduction cycle	halving production every 4 years
	Final production per block	0.0625NAC/block (reducing production for the fifth consecutive time)
	Total period	107year
	Cumulative production in the tenth year	49%
	Final block height(DPoS)	551772960
Rules Block height	1 to 20736000	1NAC/Block
	20736001 to 41472000	0.5NAC/Block
	41472001 to 62208000	0.25NAC/Block
	62208001 to 82944000	0.125NAC/Block
	82944001 to 103680000	0.0625NAC/Block
	103680001 to 551772960	0.0625NAC/Block
Income	AFN	100%
	ACN	10%

Built-in application

- NA Full Node Credentials

All nodes need to obtain full-node credentials before entering full-node working mode. Nomc and NAC need to be destroyed for certificate exchange. Specific data are as follows:

Credential number	Credential number	Destruction of nomc	Destruction of NAC	Destruction proportion	Destruction of nomc	Destruction of NAC
1–100	100	3	2851.2	0.1	300	285120
101–1000	900	3	570.24	0.1	2700	513216
1001–2000	1000	2	285.12	0.1	2000	285120
2001–3000	1000	2	142.56	0.1	2000	142560
3001–5000	2000	1	142.56	0.15	2000	285120
5001–10000	5000	1	85.536	0.15	5000	427680
10001–20000	10000	0.5	42.768	0.15	5000	427680
20001–30000	10000	0.5	21.384	0.15	5000	213840
30001–50000	20000	0.1	19.008	0.2	2000	380160
50001–100000	50000	0.1	11.4048	0.2	5000	570240

# Built-in application

NA DNS

Function definition:

I.   The user can resolve the domain name to the specified IP address for domain name binding.

II.   When the domain name is bound, need to pay the corresponding rental binding fee of 500USDN, which can be unbound and recycled after 360 days. The pledge fee will not be refunded before the expiration of the binding.

III.   The domain name needs to open the extensive analysis function can be a domain name rental binding.

IV.   Domain name rental can get income, rental needs to pay the cost of renting.

NA DFS Distributed file system

Distributed File System	
DFS Application	Each compressed file should be stored in the whole network at least 21 copies.
	Each time when replica is stored within a fixed block period, the observation node will performs a review. If it is found that there is no storage or that it cannot be opened, a vote penalty is given.

NA AppStore

01	02
App Market Purchases	App Market Release

03	04
Top apps	App Market Showcase
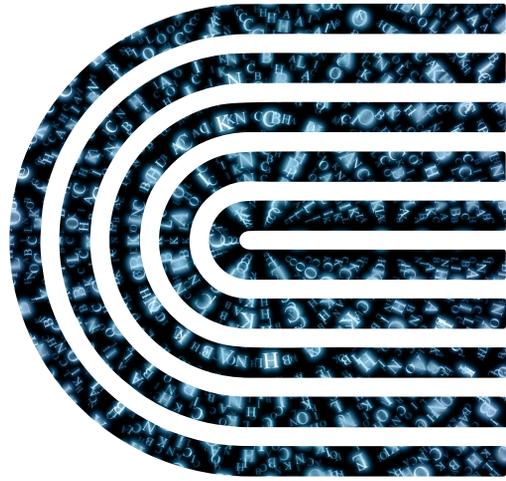
Nirvana Chain

3

Business value and application

True 100% Epic Anonymous Decentralized Application

All the DAPPs in the past weren't really decentralized because they were paid for using real names. If the author of the application does not renew the domain name or resolves the domain name, the application will not be able to open again. Another DAPP UI part of the majority is to use a Web interface for display, these all need server for storing Web interface, and the server is centralized server, it is possible by hackers to modify risk, and at the same time the author without server renewal or the server file deletion, will also result in DAPP can't work normally. In order to solve the above problems, NA public chain launched an epoch-making new concept "full hosting mode", NA public chain changed the domain name, Web interface, static resource files all into on-chain hosting mode. All the domain names are no longer their own, but rented by domain name providers all over the world. We do not need to register our own exclusive domain names, but we can rent numerous domain names on the NA platform. With this anonymous, decentralized rental approach, NA provides a completely anonymous, decentralized domain name solution for DAPP developers. It also provides a way for DAPP users to use their dapps permanently, When the author does not renew the domain name, the user of the application can renew the domain name by himself in the NA DNS platform based on the address of the application, without the consent of the domain name author. This effectively solves the concept of domain name perpetuity and every DAPP platform will have at least five domain names. In other words, as long as one domain name is still available, the application will open as normal. When a domain name does not work properly, the system will automatically reassign the new domain name to the DAPP. Make sure your DAPP always has 5 domain names available. The same is true for hosting Web resources, after the application is published, all Web resources will be synchronized to all mining nodes, ensuring that the application is backed up among all miners, thus realizing the decentralization of the application. And when the rental period arrived, ordinary users can also be renewed through the way, the site will be activated again.

New Token Contract Standards

NRC Token Contract. This Token Contract will be subdivided into Stable Coin Contract and Non–Stable Coin Contract. Among them, stablecoin contracts are divided into pledged stablecoin contracts and algorithmic consensus stablecoin contracts. Users can quickly develop their own tokens through the stablecoin contract template provided by the NA public chain.

Basic application scheme

NA public chains can be used to develop traditional DAPPs, which solves the final difficulty of decentralized applications. Implement the following application development:

Category	Description
Development type	IOS/Android application development
	DWeb application development
	Smart contracts/tokens
	Desktop software

Advanced Application Scheme

Complex applications can also be developed through the NA public chain, such as the timing task function that is not supported by all public chains at present. When a specified block is reached, the smart contract automatically triggers the corresponding function, and the processing fee consumed by this automatic trigger is from the balance of the smart contract itself. In other words, developers need to deposit a certain amount of GAS into the app in advance, or the user can deduct some fee when using the app as the GAS timing task fee in the future. With this function, we can develop very complex timed cycle tasks for complex calculations.
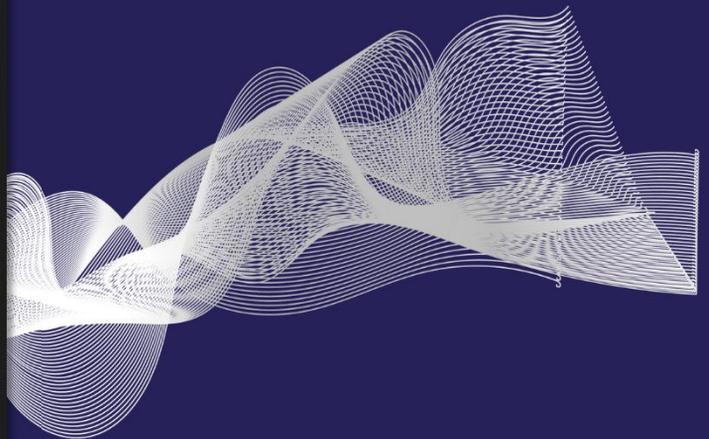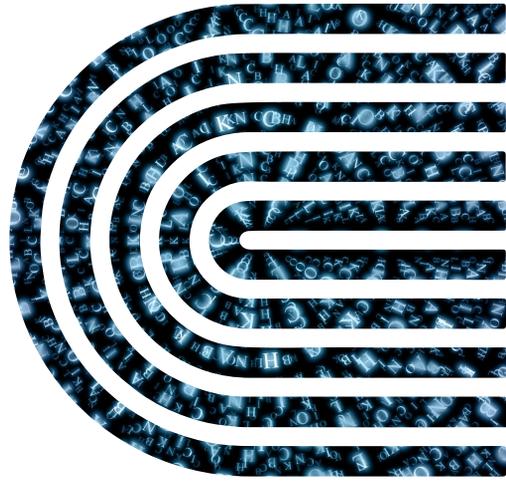
Nirvana Chain

4

Community consensus

Community autonomy establish consensus

High quality community governance mechanisms can gather internal forces, promote their own development and attract external support. After a comprehensive study of the global blockchain community, a successful blockchain community governance model needs to do the following:

First, we will establish and improve social incentive mechanisms. Only by giving enough incentives to community members can positive feedback be generated to attract more community members to join. The common incentive in the blockchain community is the "mining" activity. Therefore, in order to improve the enthusiasm of community members, the interests of all nodes must be fully guaranteed when designing community governance.

The second is full "community autonomy". The concept of "community autonomy" has become the "consensus" of the blockchain community. In practice, however, many blockchain communities are largely led by project parties. In order to fully implement blockchain community autonomy, NA Chain will adopt a distributed community model, which will be independently established by community members through voting.

The third is to practice codification. NA Chain will write the basic rules of community governance into the smart contract, which will be automatically executed by the system, and ensure the consistency and stability of community rules through reasonable allocation of governance rights. Major events and strategic decisions in the chain ecology are decided by all owners of the NA chain through consultation and voting. The governance plan of NA Chain will also be gradually improved according to the requirements of different stages of community development.

On-chain autonomy

All important parameters, rates and pricing ranges of NA Chain are decided by online voting of all nodes. Truly achieve the platform by the node consensus to maintain.

Off-chain governance

NA (Nirvana) Chain uses the DPoS mechanism. Full nodes provide the network, storage and computing infrastructure, and are responsible for the transaction verification, transaction statistics, block packaging and validation of the NA (Nirvana) Chain network. Full nodes will be rewarded for successful packaging and will also be supervised by the NA (Nirvana) Chain community. Supernodes are elected by a vote of all members of the community. Each voucher is counted as one vote, and all voucher holders can vote. Token holders will need to pledge tokens in their wallets when they vote. If the token is transferred out during this period, it will be considered a withdrawal. To ensure effective row node election, NA (Nirvana) Chain will develop a number of criteria and rules for candidates.
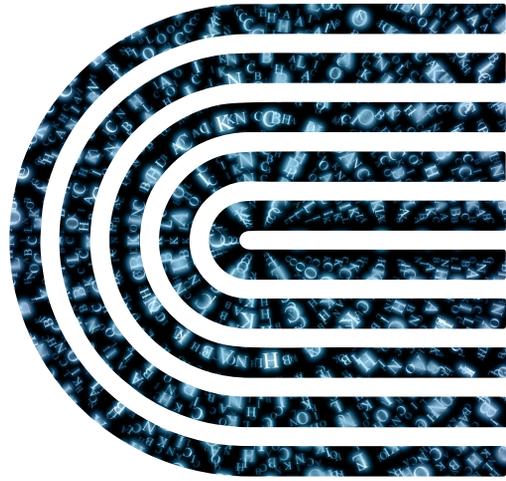
5

Ecological roadmap

Public chain carry forward plan

Stage of ecological development

Public chain carry forward plan

|	Time line	Description
Phase 0	2020 Q4	TRC20 token launch, institutional funding.
	2020 Q4	NA scheme testing and technical team establishing. Take the project to the world.
	2021 Q1	NA scheme agreement released. The first phase of NA work begins.
Phase 1	2021 Q2	Phase 1 of NA launches. Launch NVM virtual machine test data and test network release. Begin to expand the technical team and work on the second phase.
	2021 Q3	Launch mainnet, build open source community and spread awareness in tech circles, evangelize NA public chain ecosystem software and hardware scheme.
Phase 2	2021 Q4	Launch NA Phase 2 with the launch of NA USD algorithmic stablecoin. Prepare to build NA Pay's global payment platform.
	2022 Q1	xpanded NA's ground marketing and technical teams in 10 countries/regions to understand NA compensation and address customer inquiries.
	2022 Q2	Launched NA Education Service to provide R&D guidance to technicians worldwide. Work on the third phase of NA began. NA wallet is compiled on the chain, and all users can publish custom Android application APP with by NA wallet function.
	2022 Q3	NA Ecosystem establishes a parallel economy that allows for cheap and fast remittances that enable businesses to conduct transactions globally, NA Wallet is officially connected to the payment gateway merchant function.
Phase 3	2022 Q4	Phase 3 of NA begin. NA Berry OS will be released.

Stage of ecological development

Prepare   From October 2018 to September 2020, a team was formed to clarify business development needs, identify public chain design ideas, develop preliminary development and operation plans as well as complete white papers, yellow books and presentations.

Inspection   From March 2020 to December 2020, the team will advance the project according to the plan, including the development of basic components, application modules and smart contract standards, and gradually improve the relevant community governance system.

Development   From December 2020 to June 2021, the team carried out the project promotion according to the plan, including the development of basic components, application modules and smart contract standards, and gradually improved the relevant community governance system. Issuing the NRC20 Token supports an online testing chain to complete testing and upgrades. Activate the mainnet to start NA's journey of real money and build a new ecosystem. Node establishing: This includes the purchase of free node servers and the expansion of community nodes. Developer community building: Conduct publicity activities and incentive programs to attract global technology development talent.

Perfect development   From June 2021 to December 2021, improve the community, improve the ecology, promote the expansion of cross-chain and transnational business, vigorously develop the ecological community and actively promote the globalization of NA. Application establishing: When the public chain starts, the ideal state is to support no fewer than 10 killer applications and hundreds of DAPPs, and to attract more smart contracts to be deployed on the chain through hackathons and other large-scale competitions. Eco tools build: In order to improve the ease of use of the public chain, developers are provided with a variety of application projects, such as wallet, browser and development environment one-click deployment schemes, user-friendly mobile links (such as mobile devices) mobile development and contract templates.

Mature   December 2021 to December 2022, it will continue to iteratively upgrade the functions of the public chain, further deepen node construction, developer community construction, application construction, etc., and integrate the whole business of NA financial ecosystem and various types of partner assets.
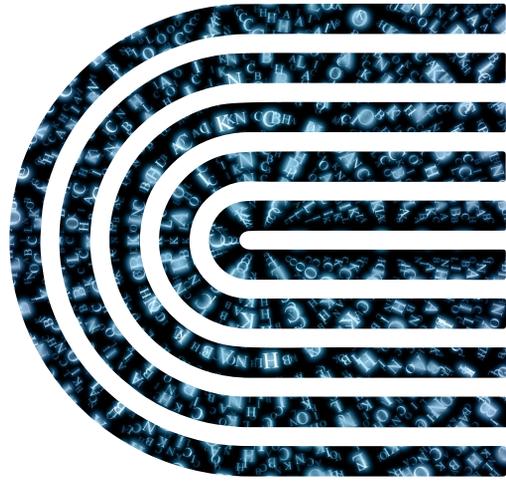
Nirvana Chain

6 ## Team information

Jonathan Lancaster

Berton Carter

Craig Thompson

Milmar Ramirez

Team information

The Nirvana Chain team has a total of 77 people. Partners spread across four continents contribute to the research and development of NA with the same values. They are distributed in Brazil, Germany, the United States, the United Kingdom, etc., including 51 blockchain technology research and development team, more than 19 people have more than four years of blockchain development experience, operation team of 17 people, public relations team of 9 people, all have more than three years of work experience in relevant fields.

The key team members with outstanding contributions will be listed below. All of them have been selected to ensure that their values are in line with the development direction of Nirvana Chain. Most of the members have worked together for many years.

Team information

Jonathan Lancaster
Chief Process Officer

Formerly Senior Mobile Development Director at Apadmi Limited

Graduated from the major of Computer Science at Oxford University. A committed blockchain cryptocurrency investor, believer, and developer. Proficient in IOS architecture, agile algorithm, blockchain and other cutting—edge technologies, committed to improve the popularity of blockchain technology and audience participation, as an excellent software engineering professional with rich relevant work experience:

From 2010 to 2011, work as a senior software development engineer at Brady, Brady PLC provides trading, risk and logistics management software solutions for the global commodities and energy markets. Working experience here accumulated a lot of industry experience.

From 2011 to 2013, worked as a front—end development engineer at HP Autonomy, where adapted to unstructured data processing and provided professional analytics tools for several well—known social media companies.

In May 2016, participated in The DAO crowdfunding launched by slock. it, and participated in The Devcon1 conference in London. After the Ethereum hard fork on July 20, some miners chose to maintain the Original Ethereum Classic (ETC).

From 2016 to 2018, affected by The DAO event, kept studying the vulnerability of recursive call SplitDAO function. And first proposed self—invocation on how to legally make smart contracts in 2018.

Since 2019, worked as a senior mobile development engineer at Apadmi, a leading mobile first digital agency in the UK, to explore the possibility of better combining blockchain technology with mobile digital technology.

From February 2019, participated in the research and development of NA(Nirvana) public chain, deeply studied the integration and innovation of technical solutions, led the technical team to design NA(Nirvana) technology and architecture, led the development of core code, and ensured the technical rationality and feasibility of the overall system architecture.

Team information

Berton Carter
Technical Manager

Former UKIC Computer Engineer

Graduated from King's College London, UK, participated in the construction of Internet network platform since 2009, and accumulated rich experience in determining project scope and reviewing project progress in cooperation with senior management. He has rich experience in making medium and long-term plans for blockchain projects, and has assisted in the formulation of global development work plans for several billion-dollar blockchain projects as well as the development and update of mobile applications, and has a think tank-level voice in the field of blockchain network platform construction, expanding user base, increasing user activity, improving product experience, and searching for appropriate profit model. Assisted UKIC to complete the development of single-chip microcomputer and baseband chip of ARM framework, and was a multi-field expert in development strategy formulation and engineering development.

Team information

Craig Thompson
DFT Engineer

Former Chief Software Engineer of CearlSwift

Graduated from Royal Holloway, University of London and has been working on crypto market blockchain since 2012. In 2017, he participated in the Sustainable Development Goals – Blockchain Study Group on 'Sustainable Supply and Demand'. Committed to using blockchain technology to solve the social industry digital trust problems. ZK–SNARK algorithm expert, has proposed a variety of block chain framework schemes, with extremely rich development experience to provide a solid support for the development progress of NA.

Team information

Milmar Ramirez
Chief Marketing Officer

NBCUniversal/Telemundo39, host, The host of Bilingual Emmy Awards

As an excellent early evangelist in the communication of blockchain industry, she has more than 30,000 followers on social media. She was invited to participate in Z.K Hackson in California as a host, and she is also an application KOL in the block chain industry in the traditional communication field. With years of experience covering and preaching about cryptocurrencies, she has a keen eye for TV live. In 2017, he won an Emmy for his NBC Universal/Telemundo 39 weather news program. In addition, she has been nominated for four awards; As a rare female leader, she is committed to injecting quality content and creating extraordinary value for the industry with her huge influence.
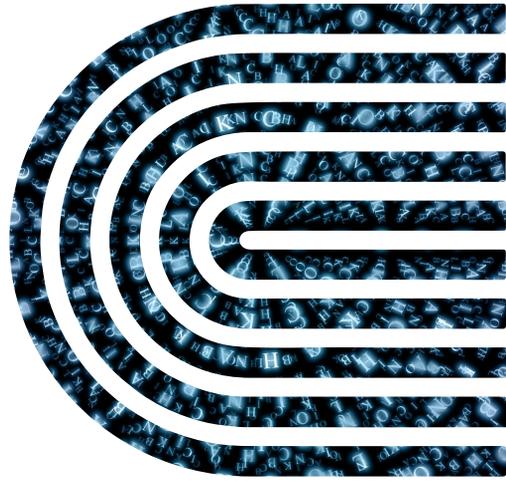
Nirvana Chain

7 Risk warning

Insufficient information

Risks associated with judicial supervision

cryptography

Development fails or is abandoned

Source code defects

Source code upgrade

competition

Token Liquidity and Price Volatility

Accident risk

Risk warning

The NA team makes no representations or warranties with respect to the NA Chain or the Project License (in particular with respect to its marketability and specific functionality) other than what is set forth in this white paper. The project should follow the principle of voluntary participation, risk, responsibility and self–financing. The development, maintenance, and operation of NA Chain are at risk, which may be beyond NA's control. In addition to the contents of this white paper, users are asked to be aware of the risks described below and to assess the ability of the parties to bear the risks described below. The development of NA Chain project may have the following risks:

Insufficient information

As of the publication of this white paper, NA Chain is still under development. Its philosophy, consensus mechanisms, algorithms, code, and other technical details and parameters may be updated and changed frequently. Although this white paper contains the latest key information on NA Chain, it is not absolutely complete and NA will be adjusted and updated from time to time for specific purposes. NA will provide community members with as much information as possible about the development of the public chain, but it cannot ensure that all information is transmitted in real time to each token holder.

Risks associated with judicial supervision

Encrypted digital assets are or may be regulated by authorities in different countries/regions. From time to time, NA may receive inquiries, notices, warnings, orders or rulings from one or more competent authorities, and may even be ordered to suspend or terminate any development or action related to the NA chain. The development, marketing, promotion or other aspects of NA Chain may be seriously affected, hindered or terminated. As regulatory policies are subject to change at any time, NA Chain's existing regulatory license in any country/region may only be temporary.

cryptography

Advances in encryption (such as cryptographic cracking) or technological advances (such as the invention of quantum computers) can pose dangers to cryptographic based systems (including NA Chain). NA cannot always guarantee the absolute security of NA Chain. To the extent reasonable, NA will take preventive or remedial measures to upgrade the underlying protocol of NA Chain to respond to any advances in encryption technology and introduce new reasonable security measures where appropriate.

Development fails or is abandoned

NA Chain is still in development, not a ready product. Due to the technical complexity of NA Chain systems, NA may from time to time face unpredictable and/or insurmountable difficulties. Therefore, the development of NA Chain may fail or be abandoned at any time for any reason (e.g. due to force majeure).

Risk warning

Source code defects

There is no guarantee that the NA Chain source code is perfect. The code may have certain defects, errors, and bugs that may prevent users from using certain functions, expose user information, or cause other problems. If such defects exist, they will impair the availability, stability, and security of the NA Chain, thus negatively affecting the value of the certificate. Open source code is based on transparency to help communities identify and solve problems. NA will work closely with the NA community to continuously improve, optimize and improve the NA Chain source code in the future.

Source code upgrade

The NA Chain source code is open source and can be updated, modified or changed by any member of the NA community from time to time. No one can predict or guarantee the exact outcome of an upgrade, correction, modification or change. Therefore, any upgrade, correction, modification or change may result in unexpected or unexpected results, which may have a material adverse effect on NA Chain's operations or the value of the Pass.

competition

The underlying NA Chain protocol is based on open source computer software. There is no claim to copyright or other intellectual property rights in the source code. Therefore, anyone can legally copy, reproduction, design, modification, upgrade and improve, recoding, reprogramming or otherwise use NA Chain source code and/or the underlying protocol, to try to develop a competitive agreement, software, system or virtual machine, virtual platform and NA Chain competition, or even surpass or replace NA Chain, NA can't control. In addition, there will be many blockchain–based competitive platforms competing with NA Chain. Under no circumstances can NA eliminate, prevent, limit, or reduce competitive efforts aimed at competing with or replacing the NA chain.

Token Liquidity and Price Volatility

Tokens are traded solely on the basis of consensus among relevant market participants about their value. No one can guarantee the liquidity or market price of a token at any time or to any extent. If a token is traded on the open market, its price can fluctuate dramatically. Such price fluctuations can be caused by market forces (including speculative trading), regulatory policy changes, 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 price of a token should be borne by the trader.

Accident risk

Blockchain technology is a rapidly developing technology. In addition to the risks mentioned in this white paper, there may be some risks that have not been mentioned or anticipated by the NA Chain team, or the various risks mentioned may occur in combination.