Ulam

A new generation of consensus innovation in the public chain area.

ABSTRACT

Ulam is the sixth blockchain project with significant innovations to the area of consensus formation, following the POW, POS, DPOS, PBFT, and DAG consensus algorithms.

The Ulam consensus algorithm was inspired by the concept of a ‘Lucky Number’ created by the famous Polish mathematician, Stanislaw Macin Ulam. The Ulam blockchain project, named after Stanislaw, uses the characteristics of the hash function to incorporate the concept of ‘Lucky Number’ to create a blockchain system with ultra-low power consumption whilst maintaining features necessary to a blockchain project, such as stability and decentralization.

Ulam does not require hash calculation competition, thereby drastically reducing the amount of work required by devices wishing to participate in the ‘mining’ process. This means that even low-power devices such as mobile phones, smart watches, and routers can participate in the ‘mining’ process which will ultimately lead to a greater potential for adaptability and growth.

Ulam’s new non-interactive transaction verification (NITCV) algorithm can effortlessly achieve a TPS (Transactions per second) of 10,000. We were able to manage these results by applying a knowledge-proven approach to algorithm design, implementing super-fragmented nodes, and avoiding computation concentration. Ulam was designed to avoid the pitfalls of other projects by implementing 49% fault tolerance, anti-quantum attack, and anti-forking features. All of these features work together to create a functional blockchain that allows for greater community adoption with a specialized consensus algorithm that can replace the POW, POS, DPOS, PBFT, and DAG algorithms.

Key words: Ulam: consensus algorithm: random number: lucky number: blockchain 3.0: non-interactive transaction verification

CATALOGUE

PROJECT BACKGROUND

As of 2019, blockchain technology has been around for 10 years. In the decade gone by, a tremendous amount of development and change has occurred in the field of blockchain technology, seeing its application and acceptance skyrocket. Bitcoin was the first realized concept of blockchain technology, however, since its inception it is far from the only player in the field. The blockchain concepts that were introduced during that time were reinvented multiple times throughout various different projects. Each project aiming to improve upon the original design of Bitcoin by focusing on improving one or more aspects of the blockchain technology itself. It's important to realize that blockchain technology has various comprising factors including peer to peer networks, cryptographic methodology, consensus mechanisms, electronic proofing and verification systems and more. This technology is essentially a decentralized distributed database that contains traceability features amongst many others.1

As blockchain technology become more widespread, the markets for these projects surged green in a generally unsustainable manner, as was seen in 2017 and early 2018. The resulting periods of market decline can be attributed to a few things, the bursting of an unsustainable bitcoin bubble, the shortcomings of blockchain technology so far, especially in the area of public chain technology, the limited number and shortcoming of applications present on the blockchain, and the limits of public acceptance for the practical use of blockchain systems.

The reason why current blockchain technologies aren't able to expand further into the application space is the lack of sufficient security, scalability, and availability that these applications would need from the infrastructure. Two of the main core technologies present in any blockchain infrastructure are cryptography and consensus mechanisms. When it comes to current consensus algorithms such as POW, POS, DPOS, PBFT, and some DAG based algorithms, there are some overbearing shortcomings which prevent them from becoming practical in nature. These shortcomings can briefly be summarized as "impossible triangles" in which the consensus algorithm prevents the blockchain technology from maintaining a simultaneous high degree of decentralization, security, stability and availability.

LOW TRANSACTION SPEED

Transaction speed, which can also be referred to as throughput or TPS (transactions per second), is an important criterion for the availability of a network system. In blockchain networks, TPS is primarily limited by the bandwidth of nodes and the consensus mechanisms implemented by the blockchain.

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

If we take a look at an already pre-established functional centralized network, the VISA 2 (Visa International Service Association) network, we can see that it has a TPS of between 5000 and 8000[2]. At this level of throughput, Visa can handle the majority of the world's credit card payment system traffic. We can then see that 5000 transactions per second are the lowest amount we should be aiming for if we are produce a blockchain payment system that can stand its ground against more traditional centralized systems.

Systems like Wechat and Alipay, which were designed to handle a much higher load of smaller transactions outpace even the VISA system in regards to throughput. Alipay for example, which uses the Oceanbase database developed by the Ant Financial group, can reach a maximum TPS of about 42,000, 000. This was enough for them to break the world record for throughput back in 2017, however, we cannot expect a general system to have or need the same throughput as Alipay's daily payment system.

A blockchain system could be applied to a high-frequency trading scenario, such as those required by IOT equipment and urban public transportation networks. For a system to be considered high-frequency, or high-throughput, It should aim to have a maximum of at least 10,000 TPS, however, we can see that this is a number that isn't present in almost all current blockchain projects. Bitcoin's network only has a TPS of 7, Ethereum can only manage 20 TPS, and EOS's TPS is only 2000. Even though EOS clearly blows Bitcoin and Ethereum out of the water in terms of stated TPS, the trade-off was is with its high degree of centralization and low robustness.

These will be discussed in further detail below, but the main point we are trying to make here is that there are no current blockchain projects that are made with high availability and TPS in mind. This is one of the most important factors holding back the application of blockchain technology today.

COMPUTATION CONCENTRATION

In a mainstream blockchain consensus algorithm such as POW and POS, mining needs to occur in order to screen transactions, incentivize participation, maintain system stability, and issue currency. The mining mechanism works by attracting 'miners' to participate in mining thereby maintaining the blockchain network, the more miners, the higher the degree of decentralization, stability and robustness the system has.

The stability of this approach can also be undermined if the concentration of power in the mining system is too high, 51% attacks and permanent divergence are examples of this. This is because the concentration of power is a centralization tendency, leading those with the most computing power to hold the greatest influence over the network.

From a computer science standpoint, the concentration of computing power will greatly impair the robustness of the entire system. From an economic and sociologic standpoint, the concentration of

[2] Fisher, Daniel (2015-05-25). "Visa Moves at the Speed of Money". Forbes. Retrieved 2016-05-01.

computing power will affect the market value of the system. It is difficult for the public to believe in a system that is easily manipulated or influenced by those with the most wealth.

In the early days of Bitcoin, Bitcoin's inventor, Nakamoto, believed that a normal laptop or desktop could serve as a bitcoin node sufficiently. If that were the case, then the entire bitcoin system would have a high degree of dispersion and robustness, and everyone would be able to participate in the mining process thus maintaining the network and distributing bitcoins relatively fairly. Unfortunately, as history has shown, this was not the case. As Bitcoin's market value rose, people invented new tools to gain the upper hand in the mining process leading to GPU mining, ASIC mining and the creation of mining pools.

As these mining machines become more commonplace and the mining pools became bigger and more established, the concentration of computing power became ever more apparent. It has become impossible for the general public to participate in the mining process, become a bitcoin node, and earn bitcoin rewards effectively amongst these heavy-weight miners and mining pools. These mining tools require so much power to generate and are so expensive to buy and keep running that they are simply out of the reach of everyday consumers.

This power centralization hinders the expansion of the bitcoin consensus and allows a few big players to potentially manipulate the bitcoin's fork and launch 51% attacks. Even though, in most cases, the owners of these mining pools wouldn't have the motivation to launch such an attack, history would show us that it's entirely possible. The Bitcoin group, which has about 51% of Bitcoin's computing power successfully manipulated Bitcoin 3 to cause a divergence and the creation of BCH[3]. These same problems also exist in Ethereum, which uses the POW consensus mechanism, and similar events also occurred with their system over the course of their history. Permanent divergences like these, manipulation of the system, and power hierarchies will severely damage public acceptance and confidence in these blockchain systems leading to a decline in the value of the currency. With this being said, the concentration of power can also be seen as a major flaw of blockchain public chain system.

HIGH POWER CONSUMPTION

Among all current blockchain public chain systems, the two most popular are the Bitcoin and Ethereum systems. Both of these systems appeared early on in blockchain history and both use the POW (Proof of work) consensus mechanism. The reasons for success of the two systems are too multidimensional and complex, so they will not be discussed in detail in this paper. However, it is undeniable that their success has a lot to do with their core consensus algorithm, the POW algorithm. This is due to the fact that the POW algorithm is currently the most consistent consensus mechanism for maintaining a high level of decentralization and stability, arguably the most

[3] Antonopoulos, Andreas (2017). Mastering Bitcoin: Programming the Open Blockchain (2 ed.). USA: O' Reilly media, inc. p. Glossary. ISBN 978-1491954386.

important features of the blockchain. If it weren't for the need for a high level of decentralization and robustness, blockchain technology could just be replaced by traditional databases in almost any application scenario.

Although POW can be fair and lead to a high degree of decentralization, it has a high level of power consumption and computational inefficiency. The mathematical basis is quite fair in nature, however, as the number of competing nodes increases, the work required to generate the necessary value increases exponentially leading to a massive consumption of power.

According to conservative estimates made by environmental groups in 2018, Bitcoin consumed about 3.3 billion kilowatts of electricity for that year, equivalent to 0.5% of the entire word's total electricity consumption. For comparison, [4] the power consumption of Denmark and Ireland combined was only 2.5 billion kilowatts for the same period of time. That means, in order to uphold and maintain the Bitcoin system for one year, 2-3 small countries worth of electricity need to be consumed, and that's not even considering the heat all the computation generates.

These consumption costs far outweigh any computer system in the world and have negative impacts on our environment that we all must bear. This is the issue with the POW consensus mechanism, and so far there is no consensus mechanism that is able to replace POW in a way that solves the energy consumption problem and maintains the level of decentralization. Current alternatives such as DPOS, PBFT, and DAG-based consensus mechanisms have solved the energy consumption problem, but they come at the cost of lower decentralization and robustness so they can't be seen as a viable substitute for POW.

CENTRALIZATION

During the early stages of blockchain technology, people began to notice the high energy consumption, low throughput and environmental effects of the POW consensus mechanism and tried to come up with various alternative algorithms in order to solve these issues. Among the solutions that were brought forward, POS, DPOS, PBFT and other DAG-based consensus all helped to fix part of the issues with the POW mechanism.

In the case of POS, it requires the mine to find a specific hash value and introduces the concept of currency age. This helped to reduce the energy consumption of the algorithm considerably when compared with its POW predecessor, however, its currency age mechanism easily induces the Matthew effect, leading to a high concentration of coins. This excessive concentration of coin distribution can destroy the entire economic system of the blockchain. So, where POS can solve one issue, it also leads to another issue, and that is the problem with the proposed solutions so far.

[4] "Bitcoin Energy Consumption Index - Digiconomist". Digiconomist. Retrieved 2018-06-08.

Other consensus mechanisms, such as DPOS, PBFT, and DAG-based consensus algorithms chose to directly eliminate the mining mechanism, thereby solving the problem of high energy consumption, but their issue is in their alternative approach. They use super nodes which handle large amounts of traffic, each of them containing between 10 and 100 of these super nodes. If these algorithms wish to offer a high TPS, they would need at least 30 of these super nodes. Due to the use of so few nodes, it's too much of a stretch to call the system decentralized, a more appropriate description would be multi-centred.

The problem with this centralization is that it leads to a low robustness of the overall system. A potential attacker could identify and launch an attack on the small number of nodes using a DDOS attack. This kind of attack has in fact happened on the EOS network in the past, and there has been attempts made using this kind of approach on the Byteball network. Some cryptocurrency experts believe that due to this centralization, these systems cannot be called complete blockchains, but rather a hybrid of blockchain and traditional multi-center server transition systems. Again, where these approaches solve the high energy consumption problem, they also introduce a new kind of issue, which is the centralization of the platform.

QUANTUM ATTACKS

Due to the fact that quantum computers being able to easily decompose large integer factors in polynomial time, these computers can be utilized to easily crack existing RSA protections. This is done using Shor's Algorithm, a quantum algorithm that can be used to solve discrete logarithm problems, as well as being used to solve current digital signature encryptions such as DSA, ECDSA, and EdDSA rendering them ineffective.

The competition to create and build usable quantum computers has already begun. Companies like Google, Microsoft, IBM, D-Wave and Intel are all racing to bring us into the quantum age. [5] Even though, as of present, there isn't a quantum computer with enough qubits to render current public key cryptography useless, experts predict we may reach this stage in 10 to 20 years' time. When such a time comes where the is a quantum computer powerful enough for this to occur, the security impact will be enormous. The security of current RSA or ECC (Elliptic Curve Encryption) algorithms will no longer be guaranteed, and the market value of blockchain systems which rely on them, such as Bitcoin and others, will collapse.

EASY FORKING

In a completely open and decentralized public chain, there should be many nodes, where each of those nodes are randomly joinable and can be removed or disconnected at any time. Only this type of system can guarantee a high level of robustness and decentralization. Public chain systems based on POW and POS meet these standards, but they face the problem whereby the problems

[5] Quantum Information Science and Technology Roadmap for a sense of where the research is heading.

presented are easily dividable.[6] Due to their open mining mechanism, it's possible for two nodes to find the random number required to obtain the packing rights at the same time (or almost the same time) which can lead to the forking of the chian.

Despite newer systems trying to avoid the occurrence of forks and lone blocks in some way, networks such as Bitcoin and Ethereum, some of the most prominent and well known blockchains around suffer from these issues. If we look at Bitcoin, we can see many coins that were forked from the original chain, notably BCH, BTG, B2X, BCD, SBTC, BCHC, and Ethereum has its forked ETC coin. These forks have resulted in many highly competitive altcoins being produced which have greatly weakened the public's confidence in the original systems as well as the market value of those systems. With that being said, the problem of forking, or bifurcation, should be avoided if the blockchain system is to stay competitive and reliable.

LOW AVAILABILITY

Usability is a vague and broad concept. In regards to blockchain systems, it refers to the extent in which a blockchain system can be used in real life. As of the chain referred to as Blockchain 1.0, Bitcoin, can be used for payment and value storage purposes only. That is to say that its usability is rather weak.

When Ethereum joined the virtual machine and implemented programmable finance, this was a great step forward, however, they lack a sufficient TPS to make the system practical in that regard rendering the chain less usable. Furthermore, the language used in Ethereum's smart contracts, Solidity, is relatively niche and complex, furthering the decline in the usability of the chain. There is also the issue of interactivity with pre-existing systems, such as Oracle, which constrains the availability and application of certain blockchain projects.

INSUFFICIENT PARTICIPATION

Generally speaking, the market value of a blockchain project relies solely on public consensus, it holds no fundamental value past this. The more people who are convinced that the chain is sufficient for its purposes, the more people care about it, the more people install the wallet and have their tokens, the higher the market value of that chain becomes. If these things don't happen then it will lead to the opposite effect, the market value of the chain dropping.

In the beginning of every project, the establishment of consensus often requires the project parties to establish a large number of communities using real money in order to develop the blockchains initial ecology. This leads the initiators and promotors of the consensus to end up becoming mere distributors of the coin. Essentially, this kind of consensus building is both high-energy and inefficient. The lack of consensus creates insufficient participation in these projects, and a dwindling

[6] Thieme, Nick (4 August 2017). "Bitcoin Has Split Into Two Cryptocurrencies. What, Exactly, Does That Mean?". Slate. Retrieved 8 March 2018.

amount of participation ultimately leads to the decline in market value of the chain. This is the issue that most blockchain projects are facing right now.

As far as the blockchain tokens are concerned, there is also a problem of insufficient participation. The only way that people can enter into the ecology of the token is by purchasing tokens, as most mining operations are out of reach for the average user. When the price of the currency rises or falls, the people holding the tokens are much more likely to sell the tokens they have on impulse and then leave the chain behind, no longer participating in any way. This of course makes it difficult to expand the blockchains reach to include more active participants. That is to say that an important factor, possibly the most important factor for total market value of a blockchain is public participation.

ULAM

Ulam is a consensus algorithm innovation project developed by the team at Tsinghua's Advanced Research Center. The consensus was inspired by the Polish mathematician Stanislaw Marcin Ulam. Stanislaw was the mathematician behind the concept of the Lucky Number, a sequence of numbers that can be algorithmically generated in a similar fashion to the generation of prime numbers and who share some similar features.

Wu Yanbing, Ph.D. in cryptography at Tsinghua University, was inspired by Ulam's work and during his research discovered that the hash function can be utilized to create a new consensus algorithm which allows for ultra-low power consumption, complete decentralization, and high stability. These Lucky Numbers helped the Ulam team to realize that reaching a consensus doesn't need to be super complicated.

Ulam doesn't need to perform a hash calculation competition which allows low-power devices, such as mobile phones, smart watches, laptops, and even routers to participate in the "mining" process. Ulam is the latest in the line of consensus algorithm innovations after such algorithms as POW, POS, DPOS, PBFT and DAG. It is also the only blockchain project in China that is made by a completely Chinese team and contains a major breakthrough for the consensus algorithm space.

The Ulam consensus is accommodating enough to be used by any super fragmented node. This means that any smart device with a connection to the internet may connect to the blockchain and participate in the mining process. Devices with minimal power and don't require much power consumption such as smartphones, laptops, tablets, can effectively take part in the mining process.

The Ulam consensus provides:

- **completely decentralization (A million nodes)**
- **prevention for a bitcoin-like computational power centralization**
- **An industry standard 49% malicious node fault tolerance**
- **A maximum TPS (Transactions per second) of more than 10,000**
- **A confirmation time of 1 second**
- **An ultra-low fork rate**
- **Protection against quantum attacks**

CONSENSUS ALGORITHM

The Ulam consensus algorithm is a redesign of past consensus algorithms and is the consensus algorithm used in the Ulam blockchain project. Our consensus algorithm determines mining operation success on the currency age of the node. The currency age of each node is a value that is generated based on the number of coins held by the node and the length of time those coins have been held. Every time a mine is mined, a set of random numbers will be produced based on the value of the currency age. The larger the currency age is, the greater the amount of produced random numbers.

The random numbers are generated using the VRF algorithm; an algorithm that ensures that the random numbers are verifiable in nature. When the block is generated, a verifiable random number is generated based on the information on the block's timestamp. If the number generated by the block at the time of mining is the same as one of the node's generated random numbers, then that node will be awarded the right to record the block. Once the node obtains the right to record a block, its currency age will be zeroed out.

This mining process is likened to the concept of a lottery, as in, the larger the currency age of each node, the more random numbers they generate and the greater their probability of matching with the block's generated random number is. The Ulam consensus algorithm can dispel the need for power-hungry and wasteful mining machines and their associated mining pools thus reducing the massive waste of resources that mining causes. Our consensus algorithm is a solid performer in regards to system performance.

From a theoretical standpoint, the TPS (transactions per second) that can be attained is infinite in nature thereby making it a good contender for a variety of scenarios including finance, transaction handling, and tracing. Ulam also guarantees the most essential point of blockchain technology, which is the decentralization of the blockchain, whilst aiming to maintain a high system throughput. We believe that the Ulam project based on our signature Ulam consensus algorithm will be the new standard of blockchain technology.

Lucky value :Ulam determines the mining probability based on the 'luck value' of the node. It doesn't need to calculate the hash value in order to do this. Each node generates a set of random numbers that will be used in the lottery process based on the luck value amount. The greater the luck value of a node, the more random numbers it will produce therefore leading to a higher probability of matching the block's randomly generated number. As previously stated, the Ulam algorithm is similar to a lottery system; the more numbers you hold, the more likely one of your numbers will match and you will be determined as the winner.

Example: Alice has a lucky value of 3, meaning she has 3 random numbers (e.g. 1, 3, and 4)Bob has a lucky value of 5, meaning he has 5 corresponding random numbers (e.g. 1, 2, 5, 7, and 8)When a block is generated, a random number is generated using the block information on the chain, for this example, we can state that the number 5 was determined. As Bob has the number 5 in his random number set, he is determined as the winner, and is the receiver of the mining reward.

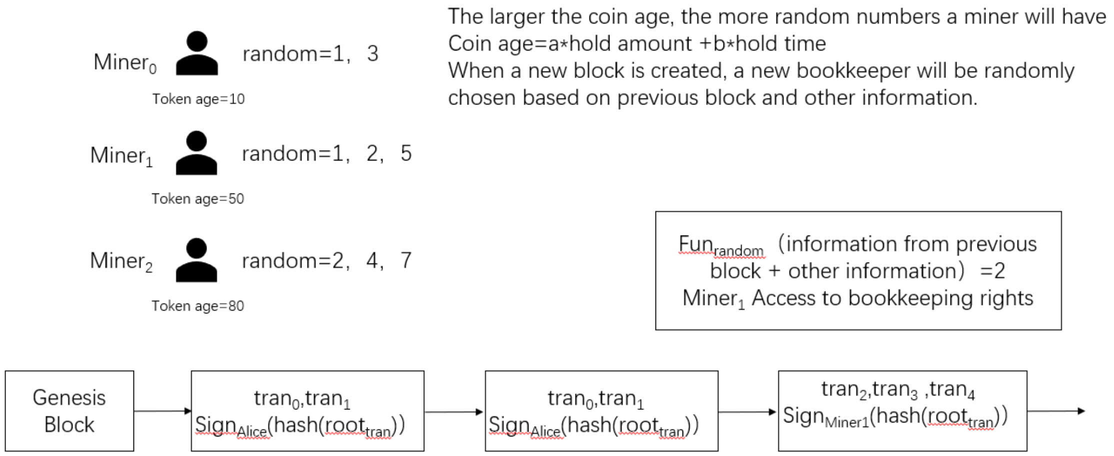

The larger the coin age, the more random numbers a miner will have
Coin age=a*hold amount +b*hold time
When a new block is created, a new bookkeeper will be randomly chosen based on previous block and other information.
Miner$_0$
random=1，3
Token age=10
Miner$_1$
random=1，2，5
Token age=50
Miner$_2$
random=2，4，7
Token age=80
Fun$_{random}$（information from previous block + other information）=2
Miner$_1$ Access to bookkeeping rights
Genesis Block
tran$_0$,tran$_1$
Sign$_{Alice}$(hash(root$_{tran}$))
tran$_0$,tran$_1$
Sign$_{Alice}$(hash(root$_{tran}$))
tran$_2$,tran$_3$,tran$_4$
Sign$_{Miner1}$(hash(root$_{tran}$))

Figure1, Consensus algorithm schematic diagram

TRANSACTIONS PER SECOND

Ulam’s new non-interactive transaction verification algorithm (NITCV) can effortlessly bring the TPS (transactions per second) of the blockchain system to 10,000 or more. This is achieved by taking a knowledge-proven approach to algorithm construction. Here, knowledge-proven refers to the proving entity persuades the verifier that his ‘knowledge’ is legitimate. The general idea is the construction of a polynomial time knowledge extractor to extract ‘knowledge’.

A normal blockchain requires all miners to verify all transactions made on the block when verifying a transaction. Ulam’s NITCV algorithm generates a transaction verification certificate after the miner packs the block and verifies the transaction within the block, thereby reducing the amount of inefficient repeated tasking leading to a greatly increased TPS. In a traditional blockchain model, where there are (for example) 1000 transactions in a block, those 1000 transactions would need to be checked by every miner to verify their authenticity, which comes at the heft price of efficiency and time-consumption.

Using Ulam’s NICTV algorithm, only one miner is required for the verification of those 1000 transactions, whilst the other miners only need to verify the proof generated by the packing node. This will effectively increase the speed of the verification process by almost 1000x over the traditional method. This kind of non-interactive transaction verification can extend the TPS of a system to a theoretical infinite amount. However, due to current day limitations of network and processor speed, the current measured TPS of the system is 10,000.

As improvement in other fields and technologies occurs, the TPS of the Ulam system will also be improved. A detailed introduction into the NITCV algorithm can be found in the Technical Yellow Book.

ANTI-COMPUTATION CONCENTRATION

Ulam has no need to calculate the hash original image in order to select the packing node, so there is no calculation competition in Ulam. Ulam calculates the lucky value of each node through a specially designed algorithm. In that way, the selection process is completely random using the luck value of the node.

With that being said, there is no benefit in having more power. For example, a supercomputer and a mobile phone would be on equal footing when it comes to the packing selection process if their currency ages are the same. As there is no gain in having more powerful equipment, the incentive for mining equipment and mining pools to be created for Ulam is gone, thereby removing the issue of calculation concentration in the Ulam system.

ULTRA-LOW POWER CONSUMPTION

As we have stated in the last section, Ulam's mining mechanism uses hash random number generation and doesn't need to look for a specific hash in order to select the packing node. The probability of a supercomputer and an ordinary smart watch finding the correct random number are the same. Due to this fact, ultra-low energy consumption can be achieved successfully and the need for power-hungry mining machines can be avoided. Any average user of smart technology (e.g. laptops, smartphones, tablets) can be an Ulam user and miner.

From our measured results, the energy consumption required for Ulam mining will not exceed 5% of the daily energy consumption on the devices used for mining. If the devices are used for 3D modelling or running games, then the impact on performance or battery will be negligible. That is to say that Ulam mining is energy efficient and doesn't require a large energy consumption of the nodes. It's suitable for solving the high pollution and energy consumption problems of the POW mechanism.

COMPLETE DECENTRALIZATION

As professional mining machines hold no advantage in the Ulam mining ecosystem, It will be unlikely that such machines will be used on the Ulam blockchain. The public will participate in mining with the use of their daily equipment, such as their mobile phones, laptops, desktops tablets, smart watches or other devices. Due to the low requirement barriers associated with operating an Ulam node, the public will be able to participate in the chain easily and actively. Even in the instance whereby a group sets up a mining pool using a large number of mobile phones, these mining pools won't have an insurmountable advantage over the average user. This will all help in the maintenance of Ulam's hardware decentralization.

This is in stark comparison with both Bitcoin and Ethereum, in whom both have very centralized mining operations due to amount of work needed to uphold the network. The establishment of these mining pools, and the high cost of specialized mining machines leaves mining well out of the hands of ordinary people with limited resources.

These mine owners, and those who decide to make money through POW based mining, have a strong incentive to continuously expand their mining pool to reduce electricity, management, and storage costs of their mining setups. This leads POW-based mining operations to have a natural Matthew causing the computing power to become very centralized. If the use of these mines weren't so prevalent, then the system would end up being much more decentralized but due to the amount of work required to mine and make a profit, this is very unlikely to occur.

If decentralized mining is to occur, it needs require lower site, management, and operating costs than a centralized mining setup. This is where Ulam shines, as the mining pools lose their advantage, more devices can be harnessed, and more users can take part in the mining, the nodes will become more decentralized in nature. If we take into account just smart phones alone, that's a potential reach of more than 10 billion nodes worldwide which would make Ulam the most dispersed and decentralized computer system in human history.

ENHANCED PARTICIPATION LEVELS

The market value of blockchain public chain projects depends primarily on the consensus of the public, and the agreement depends mainly on the number of participants and the confidence of the public. The consensus of most projects needs to be obtained through discussion, offline activities, and online publicity. This method is inefficient and has no viral spread. Once the project side stops investing real money, such projects tend to cool down.

Alternatively, once the price of the currency dramatically falls, the public will lose confidence in the project. Ulam solves this problem algorithmically. Ulam's mining mechanism is related to the age of the currency. Alternately, the probability that a mining device can obtain Ulam's primary billing rights does not depend on the computing power of the device but instead on luck and currency age. The currency age is related to the probability of digging into Ulam, and is also directly related to the amount of currency held, as well as the time of possession.

That is to say that Ulam's consensus mechanism encourages users to hold Ulam. After the price of the currency rises, the holder of the currency has incentives to not sell all of his positions at once but rather, to save part of the mined currency and continue. When the price falls, the holder has reason to refrain from selling all of the currency at once, leaving part of the currency for mining. This is because the income generated from mining can make up for the loss caused by the decline in the currency.

For new users who have no coins at all, they have the incentive to purchase a certain amount of Ulam for mining. In this way, Ulam algorithmically encourages new users to enter the market, and old users to hold positions. Ulam also gives the holders confidence in the rise and fall of currency value. These functions are all natural to Ulam and do not require the project party to continuously invest in the establishment and maintenance of the consensus.

ANTI-QUANTUM ATTACK SIGNATURE ALGORITHM

The NTRU (Number Theory Research Unit) algorithm is a public-key cryptographic algorithm invented in 1966 by three mathematics professors from Brown University in the United States. It is a cryptographic system based on a polynomial ring where N is a security parameter. Its security is based on the SVP (Shortest vector problem) in lattice-based cryptography.

NTRU holds many advantages over other public key cryptographic algorithms, such as its discrete logarithm or integer factorization and its ability to resist quantum attacks that its competitor algorithms (RSA, ECC) cannot. It is one of the main competing algorithms in the replacement of current RSA and ECC public key cryptographic systems. Other competing algorithms include the McEliece and MQ public-key cryptographic systems.

If we take a look at the other competing algorithm, the McEliece public-key cryptographic system, we can see that it is based on the error correcting code problem. This means that the algorithm is cryptographically strong, leading it to be very good at security, however, its weakness is that it's low in computational efficiency. On the other hand, the MQ (Multivariate Quadratic Polynomial) public-key cryptographic system is based on the intractability of multivariate quadratic polynomial equations over finite fields. It boasts better computational efficiency, but lacks in cryptographic strength, leading it to be less secure than its competition. The NTRU algorithm has a good middle-ground, with some advantageous features like a fast calculation speed and a smaller required storage space.

- **Key generation process:**

First we generate two polynomials randomly ($f \in Rf$, $g \in Rg$), making sure there is at least one inverse element when f mod p, or f mod q. Most values will have inverse elements if the parameter f is chosen appropriately. The inverses can be easily found by using a modification of the Euclidean algorithm. If we use Fp and Fq to present the two groups of inverse elements, then we have:

$Fq \otimes f \equiv 1 \pmod{q}$

$Fp \otimes f \equiv 1 \pmod{p}$

We then apply the calculation:

$h \equiv Fq \otimes g \pmod{q}$

Where h is a polynomial representing the public key, and f is the private key. Fp and Fq should also be hidden.

- **Encryption algorithm**

Assume m is the plaintext, $m \in Rm$

We then randomly choose a polynomial, $\boldsymbol{\phi} \in R\boldsymbol{\phi}$

Then run the calculation: $e \equiv p\boldsymbol{\phi} \otimes h + m \pmod{q}$, where the polynomial e is the cipher text.

Decryption algorithm

The private key ‘f’ can be used to decrypt the cipher text ‘e’ once we have it. Fp must be prepared beforehand.

The first step of the decryption would be: $a \equiv f \otimes e \ (\mathrm{mod}\ q)$, making sure that the factor of the polynomial ‘a’ is within $[-q/2, q/2]$

From there we can get the plaintext by doing the following calculation: $Fp \otimes a \ (\mathrm{mod}\ p)$

Decryption algorithm theory

The polynomial ‘a’ satisfies: $\in\boldsymbol{\phi}\equiv\otimes$

$$a \equiv f \otimes e \equiv f \otimes p\boldsymbol{\phi} \otimes h + f \otimes m \ (\mathrm{mod}\ q)$$

$$= f \otimes p\boldsymbol{\phi} \otimes Fq \otimes g + f \otimes m \ (\mathrm{mod}\ q)$$

$$= p\boldsymbol{\phi} \otimes g + f\ p\boldsymbol{\phi} \otimes m \ (\mathrm{mod}\ q)$$

For the last polynomial ($p\boldsymbol{\phi} \otimes g + f\ p\boldsymbol{\phi} \otimes m$), the factor of the polynomial are in the range of $[-q/2, q/2]$ if the parameter was chosen correctly. With that in mind, the result won’t be altered if we make all the factors mod q, that is to make all the factors of ($f \otimes e(\mathrm{mod}\ q)$) in the range of $[-q/2, q/2]$.

From there we can find: $a = p\boldsymbol{\phi} \otimes g + f\ p\boldsymbol{\phi} \otimes m \ (\mathrm{mod}\ q) \in Z[X]/(Xn - 1)$.

Using the polynomial ‘a’ we can calculate mod q and get $f \otimes m \ (\mathrm{mod}\ p)$. We then use Fp to multiply the polynomial we get in order to get the plaintext m.

ATTACK PREVENTION

SYBIL ATTACK

The term 'Sybil Attack' refers to the use of a small number of nodes in a peer to peer network to control a multitude of fake identities, which have the intention of causing many of the normal nodes to attack. It originally appeared in the wireless communication field. It was first pointed out that a Sybil Attack would destroy the redundancy mechanism in the distributed storage system of a peer-to-peer network. Later, Karlof and Newsome pointed out that the Sybil Attack also poses a threat to the routing mechanism in the sensor network.

Sybil Attacks can also occur in blockchain networks. However, Ulam is different. Mining in Ulam is based on the accumulation of lucky value; the generation of a lucky number depends on the information of the previous node. Therefore, even if a malicious node can create many more nodes, those nodes won't contain any lucky value because of the hash function feature. It is impossible for an attacker to forge a fake random number based on previous information. With that being said, Sybil attacks are not a concern with the Ulam chain.

51% ATTACK

Choosing the longest as the correct chain when there are multiple chains in a blockchain project is a rule of prevention of bifurcation. This mechanism choice will vary slightly for different systems, but the overall principles are similar. The generation speed of the chain is directly related to computing power. Once the attacker controls 51% of the computing power, he can arbitrarily select the bifurcation of the block he chooses and a double spend attack can be realized.

This kind of attack is called a 51% Attack. It can be similarly implemented in POW and POS systems. However, Ulam is different. When the system distributes a new block to a node in Ulam, it doesn't rely on the computing power because it is entirely random. The result is no possibility of 51% Attack in Ulam. Moreover, the generation time of a block is fixed in Ulam; the system can easily recognize the attacker's intention to double spend and invalidate the attacker’s second transaction thus preventing the double spend attack.

DDOS ATTACK

The DDoS (Distributed Denial of Service) attack refers to the combination of multiple computers as an attack platform by client/server technology to launch a DoS attack on one or more targets, thereby multiplying the threat. The central principle is to paralyze the server by the overloading of operation or bandwidth. The DDoS Attack is usually very rudimentary and crude, but often difficult to defend. Ulam prevents DDoS Attacks with using three main approaches:

- NITCV: The Ulam system can check and verify transactions through original, non-interactive transaction verification(NITCV). NITCV significantly reduces the amount of information that nodes need, and the amount of bandwidth the system requires. In doing this, it reduces the occurrence of a DDoS.

- Random Node Packing: The next node designated to be packed in Ulam is completely random making it impossible for the attacker to find the appropriate target. If the attacker cannot find the target, they cannot carry out a sufficient DDOS attack.
- High Decentralization: Even if the attacker chooses not to attack one not, but multiple nodes in a large scale attack, they wouldn't be able to attack a sufficiently large area to cause outages. That's due to the fact that the Ulam system will have so many devices participating that the attacker won't be able to effectively take down the entire network, even with massive amounts of resources. With that being said, the Ulam system is perfectly protected against DDOS attacks.

QUANTUM ATTACK

Ulam has incorporated the anti-quantum attack algorithm NTRU (Number Theory Research Unit) in its design. The NTRU algorithm is known as the fastest algorithm in the public key system. Upon inspection of this algorithm we can see that its requirements are extremely low-end; it doesn't require a computer with powerful hardware or complex hardware setups. It encompasses high speed, low demand, easy implementation, and great security which make it perfect for low power devices that seek a great amount of security with a small memory footprint.

This algorithm plays an important role in areas such as smart card technology, mobile communication systems, secure data networking, ecommerce, micro payment and authentication systems. The algorithm is paving a way in the public key space that may lead to the overall replacement of other competing algorithms like the currently popular ECDSA cryptographic system.

DELAYED ATTACK

A delayed attack in cryptocurrency is when an attacker can control the delay of a network data packet in the blockchain network in order to split the blockchain and perform a double spend action.

As the block generation time interval is fixed in Ulam, a delayed attack cannot occur on the blockchain when run in a secure environment. Undoubtedly, if the network environment is enclosed, the time system may be manipulated, however, due to the decentralization of the chain this isn't a concern.

In cases whereby the network is cross platform, border, and hardware, the difficulty required to control the time or transmission speed of the entire network is more difficult than any one individual or country could manage. With that being said, Ulam is safe against attacks of this nature.

ECOSYSTEM

VIRTUAL MACHINE

The Ulam Virtual Machine (UVM) is designed to compile smart contract code into machine code that that can be executed on the Ulam system to provide a smart contract runtime environment. It is a completely isolated sandbox environment that has no access to networks or files during runtime and limited access to other contracts.

UVM features:

- Stack-based virtual machine (as opposed to register-based) –For compiling and executing smart contracts.
- Turing Complete – A turing complete system is a general-purpose machine or programming language in which simply solves all computable problems.
- Completely isolated sandbox environment
- Stack depth of 1024 bits
- One byte of machine code – The longest stack can contain 256 opcodes.

Instructions:

All the Opcodes are defined in the file “opcodes.go”

The type of OpCode is byte. Among the result bytecodes, the first byte is the OpCode. Opcodes can be classified by 9 groups (computing related, block operation related, encryption related, etc.)

Instructions and Function Set:

There are four types of instruction sets that have been defined in the “jump.table.go” file. Each set is essentially a 256-bit length array.

The four types of instruction sets are: “Frontier Instruction set”, “Constantinople Instruction set”, “Byzantine Instruction set”, and “Home stead Instruction set” respectively. Each represent a stage of the UVM development and the instruction sets are forward compatible.

Interpreter:

The entry point has been written in the file “interpreter.go”

The smart contract can be parsed by way of the input data given by the user. It can be translated into the functions of the instruction function set, and then run.

Gas Calculation:

The two associated files are:” gas_table.go”, and “gas.go”

The way to calculate the consumed gas is context dependent. All the specific methods are defined in the gas_table file.

Smart Contract:

The contract is the storage unit of the UVM smart contract and the basic unit of the interpreter execution. This includes all the code, caller, owner, and gas-related information. (“Contract.go”)

“information.Contracts.go” contains some pre-compiled contracts for the UVM, such as ucrecover and sha256hashripemd160hash.

Memory:

“memory.go” is used for some memory operations (MLOAD, MSTORE, MSTORE8) and parameter calls (CALL, CALLCODE) in contract calls. There exists a data struct in memory in which maintains a byte array and forces functions like MLOAD and MSTORE to specify the location and length in order to accurately read and write when reading and storing data.

Stack:

“Stack.go” is the stack in UVM which is used to save operands. The types of each of the operands is big.int. When the opcode is executed, the operation parameter operand is popped from top to bottom.

Statedb:

“go-Ulam/core/state/statedb.go” is the Statedb. The contract itself does not save data. The contract and its call are similar to the database log, in which they save the contract definition and a series of operations to go with it. The current result is received by executing these operations, but as it may be too slow to execute every time, this part of the data will persist with the statedb. The two instructions SSTORE and SLOAD are defined in the code to read and write the current state of the contract from the database.

Log:

“Logger.go” is the record of UVM operation processes, memory stack statedb, and other associated records.

You may find a picture below of the logical structure of the UVM:

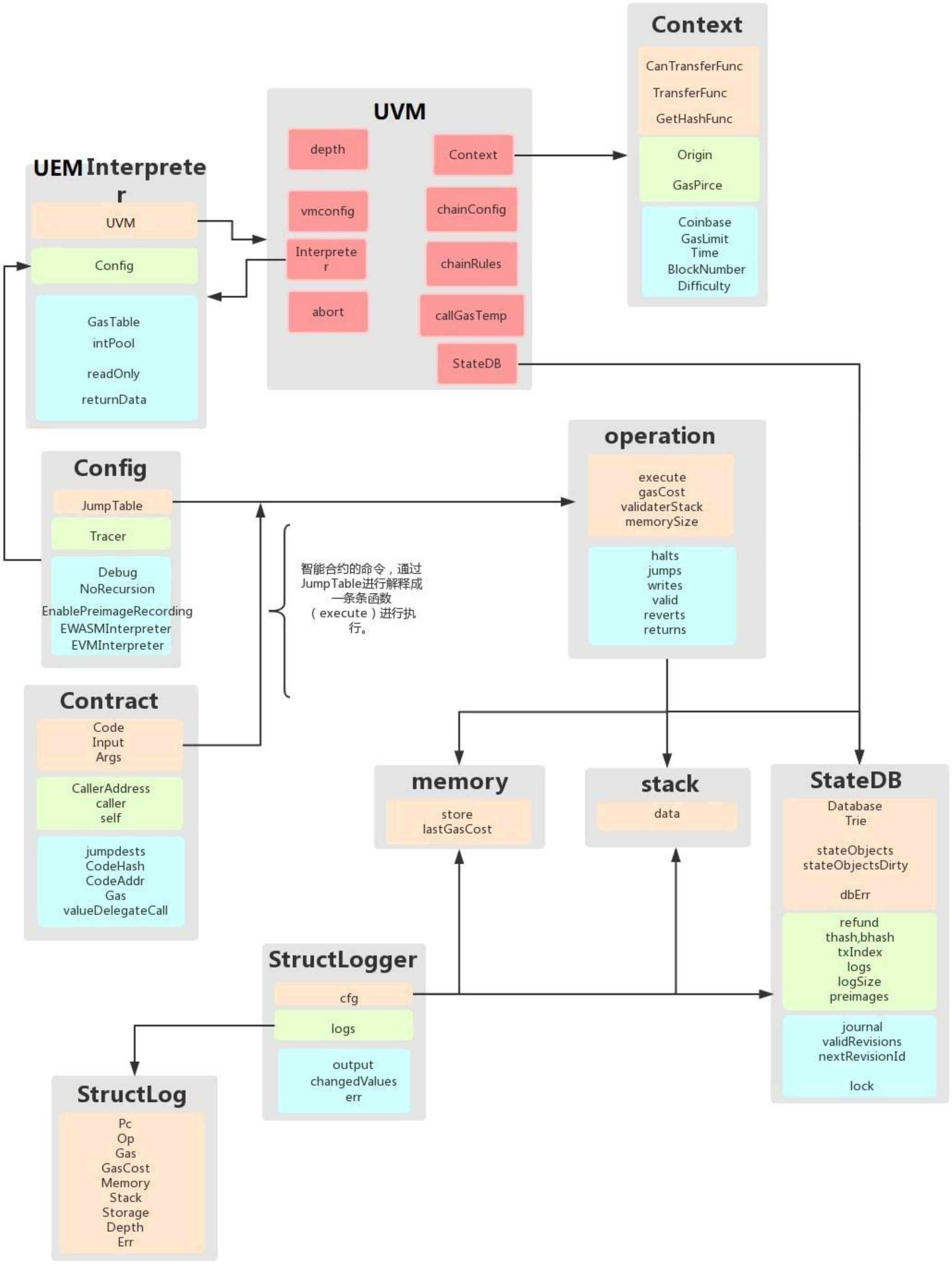


Figure 2：UVM structure chart

API

Get Account Information → GET: ulamchain.io:6000/account

Get Block Information → GET: ulamchain.io:6000/block

Get Transaction Information → GET： ulamchain.io:6000/get/transaction

Commit Transaction → POST： ulamchain.io:6000/new/ transaction

SMART CONTRACTS

The smart contract was an idea first proposed in 1994 by cryptographer Nick Szabo. According to Nick Szabo, a smart contract can be defined as a contract that executes its terms when a pre-programmed condition is met. Blockchain technology has brought the ideal decentralized, non-tamperable, highly reliable environment for which smart contracts can be utilized effectively.

Ulam has its own independent smart contract system: The Ulam Contract.

Features of the Ulam Contract:

- Certainty
- High-Performance
- Expandability

Types of Contracts include:

- Verification contracts
- Function contracts
- Application contracts

Ulam utilizes a lightweight UVM (Ulam Virtual Machine) as its smart contract execution environment which was designed to be both quick and resource friendly. The UVM is perfectly suited for small programs like those found in smart contracts. Static compilation and caching of hotspot smart contracts using JIT (Just-in-time compiler) technology can significantly improve smart contract performance.

The UVM instruction set provides a series of cryptographic instructions that optimize the execution efficiency of cryptographic algorithms found in smart contracts. In addition, data manipulation instructions support arrays and complex data structures directly. These features help to maximise the performance of the Ulam Smart Contract.

Ulam's smart contracts are highly expandable, thanks to its high-concurrency, dynamic partitioning, and low-coupling design. The low-coupling contract program runs in the Ulam Virtual Machine and communicates with the external environment by way of the interactive service layer. With this, most of the upgrades made to the smart contract function can be implemented by simply adding API's to the interactive service layer.

APPLICATION SCENARIO

The Ulam ecosystem includes the Ulam main chain, the Ulam wallet blockchain browser, virtual machines, and smart contract systems. Due to its decentralization, high TPS and security, Ulam ecology will be able to be applied to the landing of multiple scenes, putting the blockchain to the ground and indeed changing the world.

- Big Health: Ulam-based architecture can design and distribute numerous medical coins and medical blockchain platforms, meaning developers can build a big health data platform on the data chain. The platform's stakeholders include individual users, medical service providers, medical data consumers, investors, and Ulam platforms.

- The Internet of Things: Multiple logistics coins based on Ulam's archictecture can be designed and built. Utilizing the unique distributed asset transaction records and non-tamperable features of the blockchain, Ulam can effectively empower the logistics industry in five business scenarios, namely: express insured price, public benefit activities, industry blacklist sharing, express security supervision, and improvement of logistics services.

- Transportation: Ulam can be utilized in order to assist car manufacturers and shared car platforms in deploying blockchain tools that help owners with a number of tasks. Tasks may include car repair history tracking, driving behavior tracking, obtaining temporary access rights, and the recording of mileage and promotional points.

- Games: Game currencies can be designed and distributed based on Ulam's architecture. Game developers can develop games on the platform chain, and game operators can rely on Ulam for game operations. Stakeholders on the platform may include: game developers, game operators, gamers, investors, event operators, and live broadcast platforms.

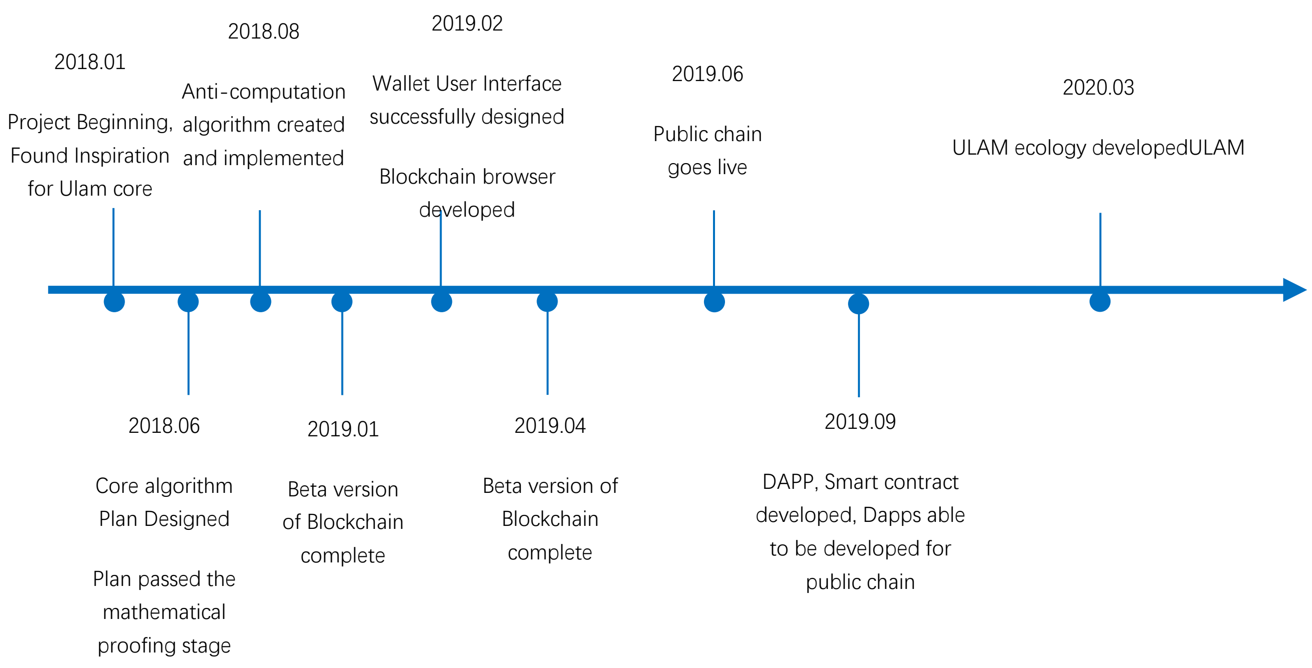
- Shared Economy: Personalized shared economic platforms may be built based on Ulam's existing architecture. The high availability and security that the chain provides is perfect for supporting the infrastructure needed for a truly shared economy.

TEAM PROFILE

Dr. Wu Yanbing is the sponsor of the Ulam project, from the Institute of Advanced studies (Mathematics) at Tsinghua University. His teacher was Wang Xiaoyun, an academic from the Chinese Academy of Sciences who cracked the Korean standard encryption algorithm LEA and proposed a new cryptographic method. His teacher has two related cryptographic papers and two patents in the blockchain field. He also helped the People's Bank of China Digital Money Institute to design a digital currency system that is both anonymous and easy to monitor. Other projects that he worked on include the creation of a credit plant platform, the design and implementation of a smart contract-based searchable symmetric encryption system, and Ethereum sidechain development.

Liu Hui is the sponsor of the Ulam community. He sold ASICMiner machines back in 2014, professionally hosted dozens of ICO projects during the ICO Roadshow in 2017, received 2 rounds of personal investment from Li Xiaolai, and incubated multiple centralization consensus projects in 2018. He is known by many through the nickname "The living fossil in the cryptocurrency field"

ROADMAP



2018.01

Project Beginning, Found Inspiration for Ulam core

2018.06

Core algorithm Plan Designed

Plan passed the mathematical proofing stage

2018.08

Anti-computation algorithm created and implemented

2019.01

Beta version of Blockchain complete

2019.02

Wallet User Interface successfully designed

Blockchain browser developed

2019.04

Beta version of Blockchain complete

2019.06

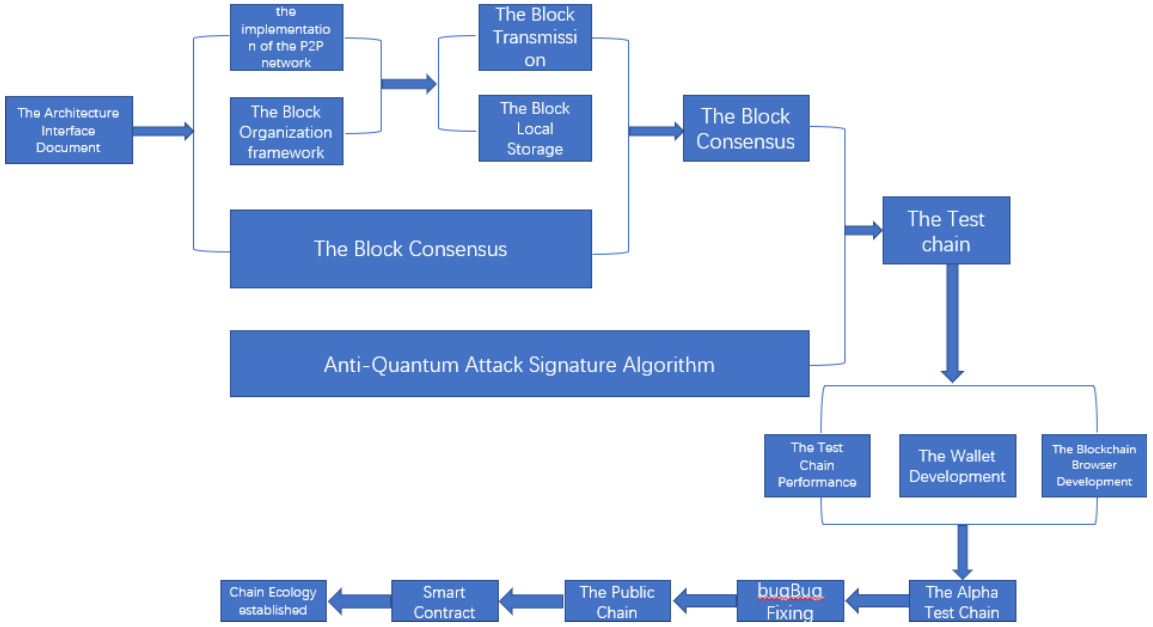
Public chain goes live

2019.09

DAPP, Smart contract developed, Dapps able to be developed for public chain

2020.03

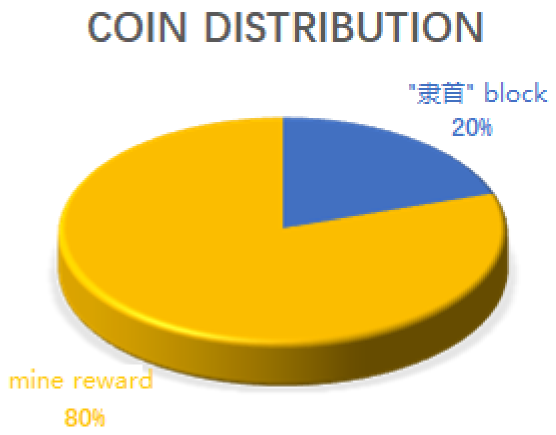
ULAM ecology developedULAM


The Architecture Interface Document
the implementation of the P2P network
The Block Organization framework
The Block Transmission
The Block Local Storage
The Block Consensus
The Block Consensus
Anti-Quantum Attack Signature Algorithm
The Test chain
The Test Chain Performance
The Wallet Development
The Blockchain Browser Development
The Alpha Test Chain
bugBug Fixing
The Public Chain
Smart Contract
Chain Ecology established

Overall development process

COIN DISTRIBUTION

The total circulation of ULAM is 1,414,213,562 pieces, which can be split to 18 decimal places. Of that number, 80% is used for mining awards with eight years of excavation; 20% is written into the "隶首" block (first block). 1,414,213,562 is an approximation of √2x1000,000,000. "隶首" is the first person to invent mathematics and bookkeeping. The original purpose of the blockchain was to bookkeep. As a way to remember and pay tribute to this great mathematician, the Ulam team chose the term "隶首 block" in order to refer the first block in the Ulam blockchain.



Around the 5th century BC, the Pythagorean school of that time focused on the study of the invariable factors in nature and society and called geometry, arithmetic, astronomy, and music, the "four arts", which were thought to pursue the harmony of the universe. They believed that everything people knew contained numbers and that it was impossible to express or understand anything without numbers.

Numbers, as far as the Pythagorean school were concerned, were only in integer form, and that fractions were the ratio of two integers. They believed that everything in the universe could be attributed as a simple ratio of integer values. A major contribution of the Pythagorean school was the proof of the Pythagorean theorem (called the “勾股定理” in China).

There was once a student of Pythagoras, Sibos, who was diligent and eager to learn, always observing analyses and thinking. He studied the problem: “Diagonal length of a square with a side length of 1” and found that the resulting answer was √2. According to the Pythagorean theorem, he found that √2 could not be represented by the ratio of 2 integers (now known as rational numbers). The incommensurability of a diagonal line and the edges of a square (the so-called commensurability of the line segment) meant that two given line segments can find a third line segment, and that the unit line segment can divide the given two line segments into integer segments.

This paradox directly violated the fundamental principles of the Pythagorean school and led to a “crisis” at the time, leading to the first crisis in the history of mathematics. Sibos, who discovered √2 did not receive glory, but rather, was severely punished and pursued by the disciples of Pythagoras. Eventually, Sibos was brutally killed by Pythagorean disciples in his attempts to escape. However, that crisis brought forward mathematics, “The language of the gods”, to another era, and thus, Sibos will always be remembered for his contribution to the world of mathematics.

√2 was the initiator of the first math crisis in history. Ulam chose this number as the circulation amount to pay tribute to Sibos, and as a wish that the Ulam consensus can trigger a revolution in the blockchain field like √2 did for the field of mathematics.

STATEMENT OF RESPONSIBILITY

This document is for informational purposes only, and is not a suggestion regarding the trading of Ulam shares or securities. Any such offer or levy will be made under a trusted clause and with the applicable securities laws and other relevant laws. The information presented above does not constitute investment decisions nor recommendations. This document does not constitute any investment advice, intention, or instruction of investment in the form of securities. This document is not intended to and be an understanding 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.

- Participation in the project means that participants acknowledge they are of the necessary age requirements and have complete civil capacity in order to participate in such a project. Once an investor participates in an investment, they adhere to the risk associated with the project, understanding and accepting the corresponding results and consequences of the investment.

- The Ulam team will continue to make reasonable attempts to ensure that the information in the white paper is truthful and accurate. During the development process, the platform may be updated, including but not limited to the platform mechanisms, the coin, the coin's mechanisms, and the coin allocation. Some of the contents in this white paper may be adjusted in the future upon project progression. Any updates made to the whitepaper by the team will be posted to the public via the project website. Participants are required to keep a copy of the latest white paper version at all times, agreeing to adjust their decisions in a timely manner based on the latest white paper. Ulam holds no responsibility for any loss as a result of: (i) Reliance on the contents of this document (ii) Inaccuracies in this document (iii) Any actions resulting from this document or its contents

- The team will spare no effort in achieving the goals mentioned in this document, but based on the existence of force majeure, the cannot make a full commitment.

- The value of Ulam relies on market rules and the needs of the application after landing. Ulam may not have any value, the team doesn't promise its value, and holds no responsibility for the consequences caused by the increase or decrease of its value.

- The Ulam platform will obey any regulations and industry self-regulation declarations that are conducive to the healthy development of the blockchain industry. Participant participation means that any inspection will be fully accepted and adhered to. At the same time, all necessary information required from the participant by any such inspection must be complete and accurate.

Others

Ulam discredits any direct or indirect losses caused by participating projects, including:

1. Economic loss due to trading operations

2.Any errors, omissions, or inaccuracies due to personal understanding

3.Any loss caused by individual transactions of various blockchain assets and any resulting behavior.

REFERENCES

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.

[2] Fisher, Daniel (2015-05-25). "Visa Moves at the Speed of Money". Forbes. Retrieved 2016-05-01.

[3] Antonopoulos, Andreas (2017). Mastering Bitcoin: Programming the Open Blockchain (2 ed.). USA: O' Reilly media, inc. p. Glossary. ISBN 978-1491954386.

[4] "Bitcoin Energy Consumption Index - Digiconomist". Digiconomist. Retrieved 2018-06-08.

[5] Quantum Information Science and Technology Roadmap for a sense of where the research is heading.

[6] Thieme, Nick (4 August 2017). "Bitcoin Has Split Into Two Cryptocurrencies. What, Exactly, Does That Mean?". Slate. Retrieved 8 March 2018.

[7] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.

[8] Robertson, Elizabeth D. (August 1, 2002). "RE: NTRU Public Key Algorithms IP Assurance Statement for 802.15.3" (PDF). IEEE. Retrieved February 4, 2013.

OTHERS

Official Website: www.ulamchain.io

Contact Email: contact@ulamchain.io