Rcoin

An Electronic Cash System for Romote Payment Scenario

http://www.rcoin.org/

CONTENTS

Introduction

In 2008, the global financial crisis broke out. At that time, the government and banks were questioned by all parties of their ability to manage the economy, and lost their credibility from the public. On November1, a mysterious crypto-geek named Satoshi Nakamoto published a Bitcoin white paper “Bitcoin: A Peer-to-peer Electronic Cash System” for the first time through a cryptography team, which caused a great sensation. On January 3, 2009, the founding block of Bitcoin was dug up and soon the first Bitcoin transfer transaction took place in the 170th block. Since then, the Bitcoin network has stepped into a flourishing era where a peer-to-peer value exchange network has been established. Until today, the overall market value of Bitcoin has exceeded trillion U.S. dollars.

With Bitcoin’s development, its underlying technological block chains have also won their place. With the help of block-chain technology, the idea of peer-to-peer value transmission is well-received. The concept of digital currency has begun to flourish in the world and has promoted the birth of a large number of digital currencies. As more and more businesses in various countries and regions begin to receive digital currency as a payment method, people are eager to enter into an era of a new currency. However, there are still many deficiencies in digital currency, including Bitcoin.

Due to lack of time for its development, the design of popular digital currencies such as Bitcoin and Ethereum is far behind the current scientific and technological development. For example, a too small block capacity is a fatal to an electronic cash system applied to payment, leading to long transaction confirmation time and inability to process a large quantity of transactions. The high transfer costs have also become a threshold that Bitcoin cannot cross in practical applications. Ethereum, as an open source block-chain smart contract platform, has frequent security vulnerabilities, threatens the security of users' information and assets, and greatly reduces users' trust in the platform. Although bitcoin and digital currencies such as Ethereum have proven us the value and great potential of block-chain technology, they are, technically, still far from the digital currency we expect to pay for.

In view of the numerous problems of current digital currency, combined with practical application scenarios, we have sought to find a solution that is better than the existing digital currency for payment application scenarios. Therefore, this article describes an electronic cash system for remote payment scenario, which we call Rcoin. Rcoin is the inheritance and continuation of concept of Bitcoin. At the same time, it compensates for some defects in Bitcoin's technology and applications. It will focus on daily life and can truly realize the payment and use of digital currency.

1. Lightening Network

Lightning network is designed for block-chain technology to adapt to massive micropayment scenarios. By establishing a micro-payment channel network for both parties to the transaction, a large number of payments from both parties can be instantaneously confirmed through slippage in multiple times, high-frequency, and bi-directionally outside the chain. When the transaction result needs to be settled, the final result is submitted to the block-chain confirmation to solve the problem of scalability of the public chain network.

The Lightning network may allow the creation of "micro-payment channels". In addition to the initial transactions that initiate channels, multiple Bitcoin transactions can be safely performed without the need to interact with the block-chain. It also does not have the risk of the counterparty: if either party terminates the cooperation, or does not respond within the agreed time, the channel can be closed. These payment transactions in the channel will be completed instantaneously and theoretically lightning network technology can achieve millions of transfers per second.

Based on the lightning network technology at this stage, Rcoin has made new optimizations to this effect, effectively preventing cost increase of commissions as users increase in number. Therefore, in implementing the Rcoin application, we regard the lightning network as an infrastructure for quick payment of the block-chain system, and implement a collaborative and interactive mode, and use flexible protocols according to different scenarios.

2. 8M Block Capacity

When Bitcoin was born, the block size was designed to be 1M, and the program stipulated that a block would be generated every 10 minutes. Obviously, with the continuous growth of transactions on the Bitcoin network, resulting in bitcoin network congestion, bitcoin confirmation slows down, transaction confirmation time becomes longer and longer, and 1M block size can no longer meet people's needs for bitcoin transactions.

In the previous market research, we analyzed the importance of block capacity for an electronic cash system. As a digital currency focused on payment usage, Rcoin’s block size is designed to be 8M. At present and in the future, the 8M block size will not have any problems with network storage capacity. Rcoin can guarantee rapid transaction confirmation capabilities in the event of large-scale transactions.

In comparison with Bitcoin, Rcoin’s transaction transfer will accelerate to a new level, which is decisive for the use of Rcoin .Only convenient and fast digital currency can fully exert its value attributes in various business scenarios.

3. Anti-quantum Attack

In the current block-chain system represented by Bitcoin, the SHA-256 hash algorithm constitutes the most basic security algorithm guarantee for the Bitcoin system, but as the quantum computer continues to make breakthroughs, especially when the Shaw algorithm was proposed, related algorithm can theoretically achieve the transition from exponential level to polynomial level. These problems that are too intractable for classical computers can definitely be solved by practical quantum computers in the future.

Quantum Resistant Cryptography (QRC) is a cryptographic system that is believed to be resistant to quantum computer attacks. The development of this kind of encryption technology is based on the difficult problem in the specific mathematics field, and it is applied in the network communication through the researches and development of algorithm so as to achieve the purpose of protecting the data security. The application of anti-quantum computation cryptography does not depend on any quantum theoretical phenomena, but its computational security is believed to be able to defend against any known form of quantum attacks.

3.1 SHA-256 Algorithm

SHA256 is one of the Secure Hash Algorithm (SHA) algorithms, whose digest length is 256 bits, i.e. 32 byte. In the bitcoin system, SHA256 algorithm is used in all places where Hash algorithm are performed.

The maximum length of the SHA-256 algorithm input message is not more than 264 bits. The input is processed in 512-bit packets. The output is a 256-bit message digest. This algorithm processing includes the following steps:

1) Add filled bits. The message is padded so that the message length is congruent with 448 modulo 512 (length = 448 mod 512), the number of bits filled is from 1 to 512, the highest bit of the padded bit string is 1 and the rest is 0.

2) Add length value. The bit length of the initial message (before padding) expressed in 64-bit is appended to the result of step 1 (the lower byte takes precedence).

3) Initialize the cache. Use a 256-bit cache to store the intermediate and final results of the hash function. The cache is represented as A=0x6A09E667, B=0xBB67AE85, C=0x3C6EF372, D=0xA54FF53A, E=0x510E527F, F=0x9B05688C,

G=0x1F83D9AB, H=0x5BE0CD19.

4) Process 512-bit (16-word) message packet sequence. The algorithm uses six basic logic functions consisting of 64-step iterative operations. Each step takes the 256-bit cache ABCDEFGH as an input, and then updates the cache contents. Each step uses a 32-bit constant Kt and a 32-bit Wt.

5) After all 512-bit packets are processed, the output of the last packet for the SHA-256 algorithm is a 256-bit message digest.

3.2 Rcoin's Anti-quantum Attack

With the development of quantum physics, the first-generation public-key cryptosystems have been successively compromised by quantum computers. These public-key cryptosystems form the anchor of the credibility chain of contemporary cyberspace. Therefore, the public focus at this stage is to quickly come up with a solution that can replace the first generation of public key cryptography and re-fix the anchor of cyberspace credibility. Although the SHA-256 algorithm used in the bitcoin network system has not found compromised security vulnerability for the moment, some potential security dangers have emerged. Faced with the constant renewal of cryptography, we need to plan ahead and build a more solid shield for Rcoin .

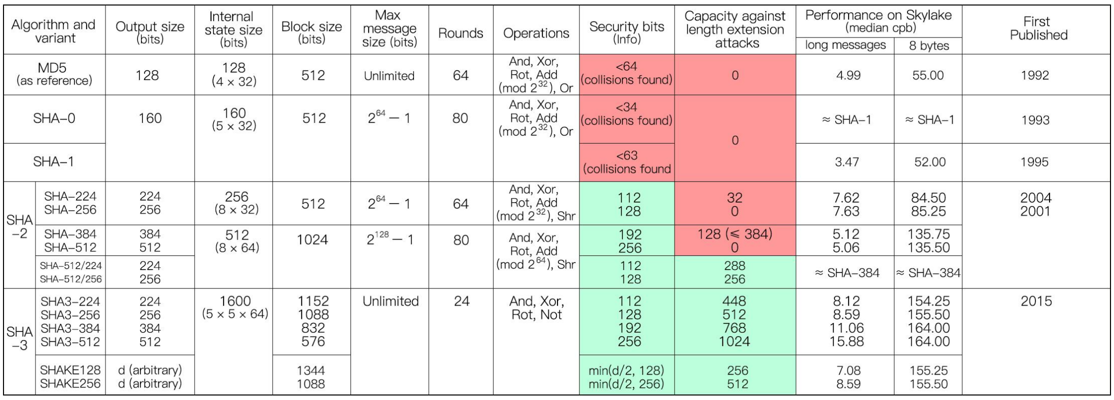
The current anti-quantum cryptography is divided into four major categories. They are Code-based Encryption (C-class), Multi-variable polynomial (M-class), Secure Hash-based (S-class) and Lattice-based Encryption (L-class). Among them, the most typical example of the S-class algorithm is the SHA-3 algorithm, which was born relatively late and did not become the US national standard until 2015.

All Hash operations in the Rcoin network system use the SHA-3 algorithm. The SHA-3 algorithm is a powerful technical reserve for Rcoin against quantum computer attacks, and it is also a highly forward-looking post-quantum technology.

3.3 SHA-3 Algorithm

SHA-3 (Secure Hash Algorithm-3) is a one-way hash function algorithm that is released as a new standard and is used as an alternative to the SHA-1 algorithm theoretically proved to be vulnerable .Companies and cryptologists around the world have submitted many SHA-3 candidates. After five years of selection, in October 2012, NIST selected the Keccak algorithm as the SHA-3 standard algorithm.

Keccak has good encryption performance and anti-decryption capability. It uses an innovative sponge function that uses XOR function to process the data with the initial internal state , which is inevitably permuted. In the largest version, the memory state used by the algorithm is to use a 5×5 two-dimensional array and the data type is 64-bit bytes, 1600 bits in total. The reduced version of the algorithm uses a relatively small, two-powered byte size w of 1 bit, 25 bits in total. In addition to using smaller versions to study cryptanalytic attacks, a more modest size (e.g. 100 bits for w=4 and 800 bits for w=32) provides a more practical and lightweight alternative.



Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (Info)	Capacity against length extension attacks	Performance on Skylake (median cpb)		First Published
										long messages	8 bytes	
MD5 (as reference)		128	128 (4 × 32)	512	Unlimited	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	0	4.99	55.00	1992
SHA–0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0	≈ SHA–1	≈ SHA–1	1993
SHA–1								<63 (collisions found		3.47	52.00	1995
SHA –2	SHA–224 SHA–256	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Shr	112 128	32 0	7.62 7.63	84.50 85.25	2004 2001
	SHA–384 SHA–512	384 512	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Shr	192 256	128 (≤ 384) 0	5.12 5.06	135.75 135.50	
	SHA–512/224 SHA–512/256	224 256						112 128	288 256	≈ SHA–384	≈ SHA–384	
SHA –3	SHA3–224 SHA3–256 SHA3–384 SHA3–512	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	Unlimited	24	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024	8.12 8.59 11.06 15.88	154.25 155.50 164.00 164.00	2015
	SHAKE128 SHAKE256	d (arbitrary) d (arbitrary)		1344 1088				min(d/2, 128) min(d/2, 256)	256 512	7.08 8.59	155.25 155.50	

Figure 1 Comparison of SHA Family Functions (From: Wikipedia)

The Keccak function is fast, with an average speed of 12.5 cycles per byte on Intel Core II processors. It is simple in design and convenient for hardware implementation. Keccak has been able to withstand a minimal complexity of 2^n attacks, where N is the size of the hash. It has a wide margin of safety. So far, third-party cryptanalysis has shown that Keccak has no serious weaknesses.

4. Workload Proof Mechanism of Anti-ASIC Mining Machine

Rcoin is a digital currency with a mining mechanism. Similar to Bitcoin, it also uses a proof-of-work mechanism. The difference, however, relies in that in Rcoin's proof-of-work mechanism, we have made numerous optimizations and improvements and given it the characteristics of anti-ASIC mining machines.

4.1 Development of Mining Industry

1) CPU mining machine

At the beginning of the birth of Bitcoin, mining mainly relied on the CPU to perform calculations. The founder of Bitcoin Nakamoto used the CPU of his computer to uncover the world's first block. At that time, due to the small number of people involved in bitcoin mining and less competition, ordinary home computers could be used for mining. The calculation power at that time was probably 20 MHash/s.

2) GPU mining machine

After some time, though the CPUs of Intel and AMD were, the miners found, more and more powerful, the computer CPU is a general-purpose processor and the CPU for graphic processing and 3D computing is much less powerful than the GPU chip. So there appeared a video card mining, which is what we call GPU mining. Through the use of video card mining, the computing ability has been greatly improved, followed by some assembled video card mining machine: the installation of multiple graphics cards on a single integrated circuit board, which is the prototype of the early Bitcoin mining machine. Since then, Bitcoin’s popularity has increased. At that time, the computing power of the graphics card was 400 MHash/s.

3) FPGA mining machine

Later, an FPGA mining machine emerged, which used an FPGA chip as the core of the calculation machine. FPGAs (Field-Programmable Gate Arrays) are products based on PAL, GAL, CPLD, and other programmable devices. It appeared as a kind of semi-custom circuit in the application-specific integrated circuit (ASIC) field, which could not only solve the deficiency of the custom circuit, but also overcome the shortcomings of the original programmable devices with a limited number of gates. During the active period of the FPGA mining machine, compared to the CPU and GPU mining machines of the same generation, the FPGA had lower power consumption and higher overall performance than the CPU of the GPU. The power of the FPGA mining machine is about 25GHash/s.

4) ASIC mining machine

The birth of the ASIC mining machine completely changed Bitcoin's ecological network and had a major impact on the entire mining industry. An ASIC (Application Specific Integrated Circuit) is an electronic circuit (chip) specially designed for a specific application. The chip used for mining is the mining machine ASIC chip. Because it is designed to perform only certain algorithms needed for mining, the design of the ASIC chip is simple and the cost is lower. But most importantly, in terms of mining power, ASIC can be tens of thousands or even more than current CPUs and GPUs in mining power. The computing power during this period also increased significantly, up to about 3.5THash/s.

5) Mine pool

With more and more people involved in mining, the computing power of Bitcoin's entire network continues to rise. It is difficult to dig up Bitcoin with a single device or a small amount of computing power, unless mine machines are brought together to form a mine pool. Thus, the mining pool came into being. The mine pool breaks through the restrictions of geographical location and gathers the miners to mine together and links mines scattered around the world. The mine pool is responsible for the information packaging, and the mine which gets access to the mine pool are responsible for the bookkeeping of competitions. Due to the collection of a lot of miners' computing power, the mine pool has a large proportion of computing power and a higher probability of digging out Bitcoin. The Bitcoin rewards generated from mining will be allocated according to the proportion of each miner's contribution. Compared to mining alone, adding a pool can provide more stable benefits. At present, the globally more powerful pools include fish ponds, ant pools, currency nets, national pools, and BitFury .With the exception of BitFury, the rest come from China.

4.2 Rcoin's Mining Algorithm

To solve the problem of mining specialization and computational concentration caused by mining machines including the ASIC ones, Rcoin uses the Equihash algorithm .The Equihash algorithm was invented by Alex Biryukov and Dmitry Khovratovich and its theoretical basis comes from a well-known problem in computational science and cryptography—the problem of generalized birthday paradox. Equihash has a very effective validation mechanism. This is very important for the implementation of light clients (Rcoin mobile light wallets) on future limited-function devices .

Equihash is a proof of workload that requires high memory, which means that how much money you can dig depends primarily on memory size. This also means that no one is likely to establish cost-effective custom hardware (ASIC) for mining in the foreseeable future, and Equihash's main optimization cannot give miners a mining advantage. The use of the Equihash algorithm can avoid the concentration of mining processes in the hands of several first-rate miners based on specialized mining hardware, thus contributing to the "democratization" of digital currency.

Compared with most other digital currencies, Rcoin has brought Equihash, the most academically advanced encryption algorithm, to make the mining process more decentralized, lowering the threshold for mining, and facilitating the creation of a nation-wide mining era.

5. A More Secure Signature Algorithm

5.1 ECDSA Signature Algorithm

In the bitcoin system, the ECDSA signature algorithm is used with the ECC scheme where encryption is not used in the core implementation but only signature algorithms to ensure transaction authenticity and ownership authentication.

1) An Overview of ESDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a simulation of a digital signature algorithm (DSA) using elliptic curve cryptography (ECC). Unlike the ordinary discrete logarithm problem (DLP) and the integer factorization problem (IFP), the elliptic curve discrete logarithm problem (ECDLP) has no sub-exponential time solution. Therefore, the unit bit strength of elliptic curve cryptography is higher than that of other public key systems.

The Digital Signature Algorithm (DSA) is discussed in detail in the Federal Information Processing Standard (FIPS) , known as the digital signature standard. Its security is based on the discrete logarithm problem on the prime domain. The elliptic curve cryptosystem (ECC) can be seen as an elliptic curve modelling a previous cryptosystem based on the Discrete Logarithm Problem (DLP), except that the group elements are replaced by the points on the elliptic curve over the finite field from the number of elements in the prime domain. The security of elliptic curve cryptosystem is based on the elliptic curve discrete logarithm problem (EDDLP). The discrete logarithm problem of the elliptic curve is far more difficult to solve the discrete logarithm problem. The unit bit strength of the elliptic curve cryptosystem is much higher than the traditional discrete logarithm system. Therefore, in the case of using a shorter key, the ECC can reach the same security level as the DL system. This brings the benefits of smaller computational parameters, shorter keys, faster computing, and briefer signatures. Therefore, elliptic curve cryptography is especially suitable for occasions of limited processing ability, storage space, bandwidth and power consumption

2) Principle of ECDSA

ECDSA is a combination of ECC and DSA. The entire signature process is similar to DSA, but the algorithm used in the signature is ECC, and the final signed value is divided into r and s.

The signing process is as follows:
1. Select an elliptic curve Ep (a, b) and the base point G;

2. Select the private key k (k<n, n is the order of G) and use the base point G to calculate the public key K=kG;

3. Generate a random integer r (r<n) and calculate point R=rG;

4. Set the original data and the coordinates of x and y of the point R as a parameter and calculate SHA1 as hash, i.e. Hash= SHA1(original data, x, y);

5. Calculate s≡r-Hash*k (mod n);

6. Set r and s as the signature value and if either is 0, re-start the process from the third step.

The verification process is as follows:

1. After receiving the message (m) and the signature value (r, s), the receiver performs the following operations;

2. Calculate: sG+H(m)P=(x1,y1),r1≡x1 mod p.

3. Verify the equation: r1≡r mod p.

4. If the equation is established, accept the signature, otherwise the signature is invalid.

3) Disadvantages of ECDSA

- **Side channel attacks**

Although the encryption algorithm has been improved, the security of the encryption system is still the focus of the secret system design. Side channel attacks can exploit the physical flaws of the encryption system to obtain confidential information. In October 2016, a research team from the University of Tel Aviv used electromagnetic attacks to analyze the security of several common password databases in the Apple iOS system and discovered several weaknesses that could be exploited by side-channel attacks, and successfully restored the key implemented by ECDSA in OpenSSL and CommonCrypto libraries.

This means that there are still physical flaws that can be attacked in the ECDSA algorithm, and it is very likely to become the attack point by hackers.

- **Malleability attacks**

In each signature, there is exactly one DER-encoded ASN.1 octet representation, but OpenSSL is not enforced. As long as a signature is not changed entirely, it is acceptable. In addition, for each ECDSA signature (r,s), this signature(r, -s(mod N)) is a valid signature of the same message.

The ECDSA algorithm generates two large integers r and s and combines them as a signature, used to verify transactions, which is the principle of malleability attacks. And r and BN-s can also be used as a signature to verify the transaction (BN=0xFFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141). Thus, the attacker obtains a transaction, extracts the r, s of the inputSig, uses r, BN-s to generate a new inputSig, and then composes a new transaction with the same input and output but different TXIDs. Legitimate transactions can be successfully generated by attackers at almost no cost without a private key.

Malleability attacks do not prevent the actual transaction from being sent, but the confirmation by the network is not necessarily the original expected TXID. This has also become one of the major threats of ECDSA.

5.2 Ed25519 Algorithm

Compared to the ECDSA algorithm used in bitcoin signature systems, Rcoin uses a faster and more secure Ed25519 signature algorithm.

Ed25519 is a public key signature system with several attractive features:

Fast single-signature verification. The system only needs 273364 cycles to verify the signature on Intel's widely deployed NealeMe/Westmere line CPU. (This performance measure is for short messages. For very long messages, the verification time is mainly controlled by the hash time.) Nehalm and Westmere cover all the cores including the CPUs of I7, I5 and I3 released between 2008 and 2010, as well as most Xeon CPUs released during the same period.

Faster batch verification. The system performs 64 individual signature verifications (verifying 64 signatures of 64 messages in 64 public keys) in only 8.55 million cycles, i.e. 134,000 cycles per signature. The software easily fits into the L1 cache, so the competition between the cores is negligible: a quad-core 2.4GHz Westmere verifies 71,000 signatures per second while maintaining a maximum verification latency of less than 4 milliseconds.

Fast signing. The system can sign a message with only 87,548 cycles. The quad-core

2.4GHz Westmere sends out 109,000 messages per second.

Fast key generating. Key generation is almost as fast as signatures. There is a slight penalty for key generation to obtain secure random numbers from the operating system; dev/urandom under Linux takes about 6000 cycles.

High security level. The system has a security goal of 2^{128}; it overcomes the similar difficulties of NIST P-256, RSA and 3000-bit keys, and 128-bit packet passwords enhancement. The current worst attacks actually spend on average more than 2^{140} bits of operation, and as the number of bit operations drops, they degrade twice in the probability of success.

Infallible session key. Signatures are generated deterministically; key generation consumes new randomness, but new signatures do not. This is not only a speed feature, but also a security feature that is directly related to the recent crash of the Sony PlayStation 3 security system.

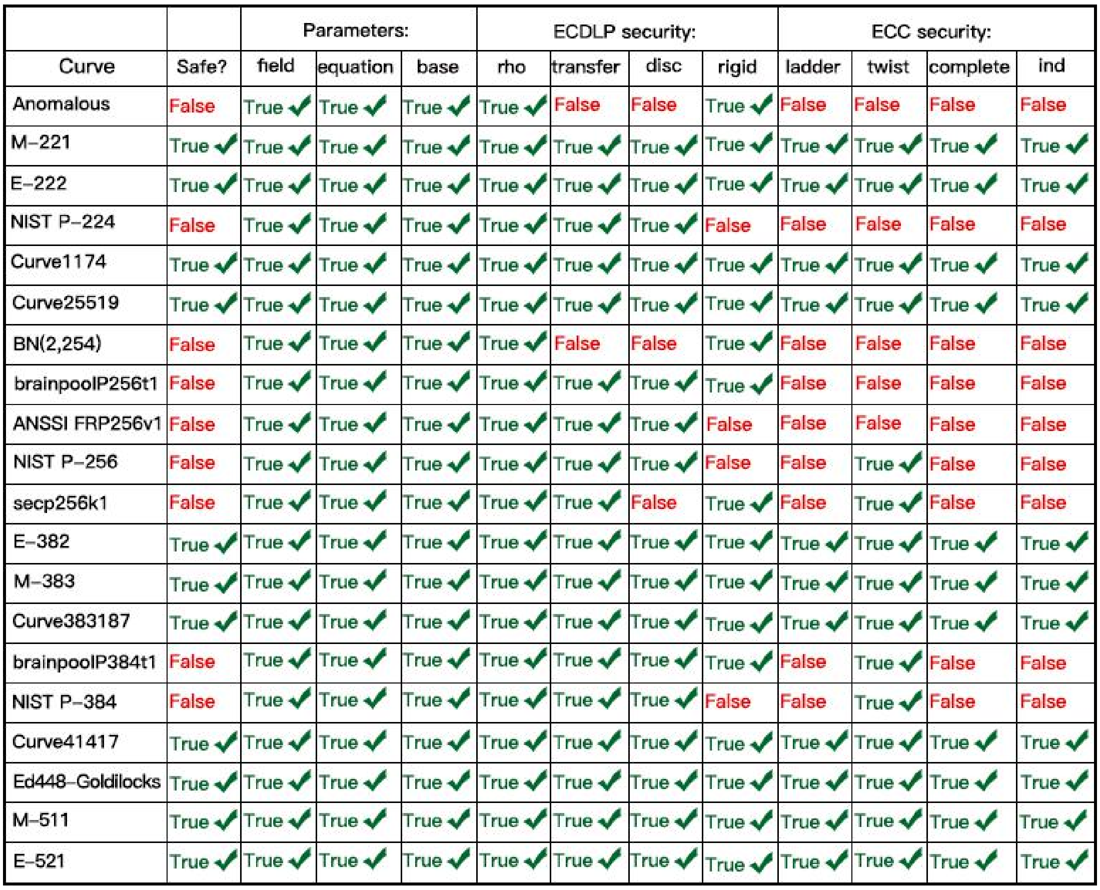
Collision elasticity. Hash function conflicts do not break the system. This adds a layer of defense to the weak points in the selected hash function.

No secret array index. The system does not read or write data from the secret address in RAM. The address pattern is completely predictable. Therefore, the system is not affected by cache timed attacks, hyper-threading attacks, and other side channel attacks that rely on address leaks through the CPU cache.

No secret branch conditions. The system never performs conditional branching based on secret data; the skipping mode is completely predictable. Therefore, the system is not affected by side channel attacks though information leakage by branch prediction unit.

Small signature. The signature is suitable for 64 bytes. These signatures are actually compressed versions of longer signatures; the time for compression and decompression is included in the number of cycles described above.

Small key. The public key takes only 32 bytes. The time for compression and decompression is once again included.



		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False	False	False
M-221	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
E-222	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
NIST P-224	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False	False
Curve1174	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
Curve25519	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
BN(2,254)	False	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False	False	False
brainpoolP256t1	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False
ANSSI FRP256v1	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False	False
NIST P-256	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False
secp256k1	False	True ✓	True ✓	True ✓	True ✓	True ✓	False	True ✓	False	True ✓	False	False
E-382	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
M-383	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
Curve383187	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
brainpoolP384t1	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	True ✓	False	False
NIST P-384	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False
Curve41417	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
Ed448-Goldilocks	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
M-511	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
E-521	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓

Figure 2 Curve Security Requirements Decomposition (From: Secure Curve Website)

The Ed25519 signature is an elliptic curve signature that has been carefully designed and implemented at multiple levels of design to achieve very high speeds without compromising security. Rcoin uses the Ed25519 signature algorithm to keep the entire signature system safe and fast while maintaining a good performance.

6. The Total Amount of Distribution and Mining Mechanism

The total number of Rcoin releases was 10 million, of which 1 million were for gifts and 2 million were produced through mining .

In order to promote the development of the Rcoin network system in terms of incentives, Rcoin has adopted a workload proof mechanism against ASIC mining machines. The specific technical parameters are as follows:

Block time: 10 minutes
Total mining time: 106 years
First halving cycle duration: 3.8 years
The first halving cycle per block output: 5 RCO

The first halving cycle output of the total mining: 50%
Adjustment period for difficulty: 2 days

The Rcoin wallet was officially launched on the Rcoin official website (www.rcoin.org) at 20:00 on April 20, 2018. In view of Rcoin's mining algorithm, users can download Rcoin wallets for mining through ordinary domestic computers.

7. Rcoin's Application

Rcoin is an electronic cash system for remote payment scenarios. It is mainly used for payment services between multinational businesses, international finance, and various financial institutions. Rcoin is an open blockchain-based payment platform system that focuses more on larger payments. In the payment system built by Rcoin, the payment service is handled in a one-by-one manner in real time to achieve full liquidation. The purpose of our system is to provide fast, efficient, secure and reliable payment and liquidation services for all businesses and financial markets on a blockchain basis, as well as for business transactions between different countries and regions. It greatly reduces the risks and avoids the loss of any of the parties due to factors such as exchange rates.

8. Conclusion

We have proposed an electronic cash system for remote payment scenarios in this article. Compared to Bitcoin's technical deficiencies, Rcoin is a more sophisticated and optimized electronic digital currency that gives more possibilities for realizing applications in specific scenarios. In order to solve the problem of high transaction fees and transaction confirmation time for Bitcoin, Rcoin adopts an 8M block capacity, combined with lightning network technology, to achieve a dramatic increase in transaction transfer speed. In the face of security risks in existing digital currencies, Rcoin uses the SHA-3 algorithm that resists quantum attacks and the faster and more secure Ed25519 signature algorithm. At the same time, by reviewing the development of the mining industry, especially the gradual concentration of mining calculations, we have given the Rcoin mining mechanism with anti-ASIC mining machine features in a technical way, which helps to achieve the "democratization" of digital currency. In short, Rcoin will be a better proposition for digital currency.