MKcoin

White Paper

SUMMARY

Bitcoin has successfully implemented the concept of p2p e-cash. Both professionals and the public recognize the ease of combining public transactions and work as a model of trust. The electronic cash user base has grown steadily today. Customers are attracted by low fees, and the anonymity provided by e-cash and merchants values

their forecasts and emissions. Bitcoin effectively proves that electronic cash can be as simple and convenient as banknotes and credit cards. Unfortunately, Bitcoin has encountered several flaws. For example, the distributed nature of the system is inflexible, preventing the implementation of new features until almost all network users update their clients. Some key flaws that cannot be resolved quickly prevent the spread of Bitcoin. In such an inflexible model, launching a new project is more efficient, rather than permanently repairing the original project. In this paper, we have studied and proposed a solution to the main defects of Bitcoin. We believe that systems that take into account our proposed solutions will lead to healthy competition between different e-cash systems. We also present our own electronic cash "CryptoNote", a name that emphasizes the next breakthrough in e-cash.

We investigated the main pitfalls of Bitcoin and proposed some possible solutions. These advantages and our ongoing development have made the new electronic cash system CryptoNote a serious rival to Bitcoin, surpassing all forks. Nobel laureate Friedrich Hayek proved in his famous work that the existence of an independent currency has a huge positive effect. Every currency issuer (or developer in our case) is attracting users by improving his products. Money is like a commodity: it can have unique interests and shortcomings, and the most convenient and trustworthy currency has the greatest demand. Suppose we have a comparative advantage currency: this means that Bitcoin will grow faster and become better. The biggest support for open source projects comes from users who are interested in it. We don't think CryptoNote is a complete replacement for Bitcoin. Conversely, having two (or more) powerful and convenient currencies is better than just one.

Chapter 1 Blockchain

1.1 Blockchain technology origin

Blockchain technology originated in 2008, the groundbreaking paper "Bitcoin: A Peer-to-Peer Electronic Cash System" published by the scholars named "Satoshi Nakamoto" in the cryptography mailing group. In the past two years, the research and application of blockchain technology has shown explosive growth. It is considered to be the fifth subversive innovation in the calculation method after mainframe, personal computer, Internet, mobile/social network, and is the evolution of human credit. In the history of the fourth milestone after blood credit, precious metal credit, and central banknote credit. Blockchain technology is the prototype of the next generation of cloud computing. It is expected to completely reshape human social activities like the Internet and realize the transition from the current information Internet to the value Internet.

1.2 Blockchain

Blockchain is a kind of database structure that combines blocks in a chain. It is suitable for storing simple, sequential data that can be verified in the system. It is guaranteed by cryptography that data cannot be falsified or counterfeit. He is able to enable participants to formulate formulas for the sequence of events and current state of the entire network transaction record.

Data angle

A distributed database that is almost impossible to change.

"Distributed" features:

1. Distributed storage of data: stored in all nodes participating in the recorded data, not stored centrally in the centralization node.

2. Data distributed records: system participants maintain together.

Effect angle

Record time-critical, non-tamperable, and trustworthy databases;

This "database" feature:

Decentralized storage; data security and effective guarantee.

Technical perspective

A variety of prior art integrations (such as encryption algorithms, P2P file transfers). These technologies are combined with databases in new structures to create a new way to record, deliver, store and present data.

1.3 Blockchain Infrastructure Model

The blockchain system consists of a data layer, a network layer, a consensus layer, an incentive layer, a contract layer, and an application layer. The data layer encapsulates the underlying data block and related data encryption and time stamping technologies; the network layer includes a distributed networking mechanism, a data propagation mechanism, and a data verification mechanism; and the consensus layer encapsulates various types of consensus of network nodes. Algorithm; the incentive layer integrates economic factors into the blockchain

technology system, mainly including the issuance mechanism and distribution mechanism of economic incentives; the contract layer mainly encapsulates various scripts, algorithms and smart contracts, and is a blockchain programmable feature. The foundation; the application layer encapsulates various application scenarios and cases of the blockchain. In this model, time-stamp-based chain block structure, distributed node consensus mechanism, consensus-based economic incentives, and flexible programmable smart contracts are the most representative innovations of blockchain technology.

1.4 Blockchain - Features

1, open, consensus

Anyone can participate in the blockchain network, each device can act as a node, and each node is allowed to get a complete copy of the database. The nodes are based on a set of formula mechanisms to jointly maintain the entire blockchain through competitive computing. If any node fails, the remaining nodes will still work.

2, go to the center, go to trust

A blockchain consists of a number of nodes that together form an end-to-end network. There are no centralized devices and authorities. Data exchange between nodes is verified by digital signature technology, without mutual trust. As long as the rules are established according to the system, nodes cannot and cannot deceive other nodes.

3,Transaction is transparent and both parties are anonymous

The rules of the blockchain are open and transparent, and all data information is public, so each transaction is visible to all nodes. Since nodes and nodes are trusted, there is no need to disclose identity between nodes, and each participating node is anonymous.

4, can not be tampering, traceable

Modifications to the database by a single or even multiple nodes cannot affect the database of other nodes, unless it is possible to control more than 51% of the nodes in the entire network to modify at the same time, which is almost impossible. So it can be traced back to the past and present of any transaction.

1.5 Blockchain - Three core issues

1. How to record and store this rigorous database, so that even if some nodes participating in data logging crash, can we guarantee that the entire database system is running properly?

2, how to establish a rigorous database, so that the database can store a large amount of information, while at the same time can maintain the integrity of the database in a system without a centralized structure?

3. How to make this rigorous and complete database become trustworthy, so that we can prevent fraud on the Internet without real name background?

1.6 Blockchain - Four Core Technologies

Block + chain

For question one, the blockchain solution is:

Innovate the structure of the database, divide the data into different blocks,

each block is linked to the back of the previous block by specific information, and is connected in order to present a complete set of data.

Distributed structure

Problem 2 solution:

The blockchain structure design allows each node participating in the data transaction to record and store all the data.

Asymmetric encryption algorithm

In the blockchain system, the basis of the ownership verification mechanism is the asymmetric encryption algorithm.

script

Script - a programmable smart contract. In the decentralized environment of the blockchain, all protocols need to reach consensus in advance, and the introduction of the script is indispensable.

1.6 Blockchain Application Scenario

Cross-border payment – this involves the conversion of foreign currency, the foreign currency must be settled during the conversion process, which leads to a foreign currency cross-border payment, often more than a few days, and blockchain technology may be in a matter of seconds carry out.

Legal deposits – There are many legal evidence documents that do not wish to be tampered with, and blockchains can prevent data from being tampered with.

Social and gaming – The best direction in traditional Internet business is social and gaming, and natural is an interactive property. Blockchain has a very

good natural advantage for the community, so blockchain technology can be used in many scenarios, especially in games and social applications.

Supply Chain Finance - Because it involves the detailed trust of all parties, and the blockchain is just a trust mechanism, this is a suitable application scenario.

Authentication - protects your personal privacy data.

Energy – for example, in some countries in Europe and America, a large number of distributed solar energy and distributed wind energy are encouraged. The excess energy of the community and the community can be shared. This is a typical concept of energy sharing.

Media content information - This piece is a strong incentive for original content. The blockchain can be used to share the ID of the original content in the form of profit sharing. Therefore, the blockchain is naturally in the social media, media or in some entertainment industries, such as music, small video industries, blockchain technology can also play a big role.

Product traceability - I think the product traceability is paradox in some sense, because the blockchain can only guarantee that the above data has not been tampered with, but the original data has not been tampered with. Therefore, it depends on the technical means of the Internet of Things to guarantee, but it is combined with the blockchain, rather than saying that the blockchain alone helps traceability.

Anti-counterfeiting of works of art or collectibles - In fact, high-value works of art and collectibles have very strong financial attributes in a certain sense. Since

there are strong financial attributes, the blockchain can do some traceability on anti-counterfeiting. At the same time, an indivisible piece of art in real life can be made into an infinitesimal division through the form of a pass.

1.7 Blockchain development history

In 1991, Stuart Haber and W. Scott Stornetta first proposed encryption protection products for blocks.

In 1998, Nick Szabo conducted a research on the mechanism of electronic money decentralization. He called this bit gold.

In 2000, Stefan Konst published a unified theory of encryption protection chains and proposed a set of implementation plans.

In 2008, the concept of blockchain was first proposed by Nakamoto.

The 2014 blockchain "2.0" became a term for decentralized blockchain databases

In 2016, the Central Securities Office of the Russian Federation (NSD) announced a pilot project based on blockchain technology.

The introduction of blockchain technology **in 2018** indicates the arrival of the "3.0" era of blockchain.

1.8 Blockchain Chain Technology

Why use sub-chains? Is the current smart contract not very good?

Existing smart contracts have provided a Turing-complete solution that is powerful

and can be customized to be written in a blockchain system. However, with the continuous warming of blockchain technology and the gradual landing of applications, the problem of the underlying platform of blockchain based on smart contracts is becoming more prominent. The most criticized is the low transaction speed and poor scalability, which cannot meet large-scale commercial application scenarios. In addition, the transaction cost is too high, and it is also a problem that cannot be evaded by large-scale construction applications.

So what is a child chain? A sub-chain refers to a blockchain with independent functions derived from the platform of the main chain. These sub-chains cannot exist alone, must be run through the infrastructure provided by the main chain, and all users of the main chain are freely available. Unlike the parallel operation of the side chain and the main chain, the sub-chain is concentric with the main chain mother and child, and the attack sub-chain alone has no effect. The technical path of the sub-chain not only solves the security problem of the side chain, but also provides a series of powerful functions. It also marks the blockchain 3.0 era in which the blockchain entered the sub-chain technology from the 2.0 era of Ethereum.

Why use sub-chains?

First, the sub-chain implements the scalability of the blockchain system,

providing a practical solution to blockchain fragmentation.

Because it is a very difficult problem to solve fragmentation on a single blockchain. For a smart contract, we deploy it as a sub-chain, and only save the internal state of the contract inside the sub-chain. It does not need to store the specific information of the contract application on the public chain, which greatly relieves the storage pressure of the main chain. High-parallel processing through sub-chains greatly reduces the processing bottleneck of the main chain.

Second, the sub-chain provides great flexibility

The first is the flexibility of the consensus approach. The consensus mode of a single blockchain is fixed after deployment. For example, the consensus method of Bitcoin is POW. When deploying applications (DAPP) based on this, you cannot choose other consensus methods. For example, the new application scenario wants to use a fast POS consensus method. Because the consensus of the underlying public chain has been fixed, this problem cannot be solved. However, the sub-chain function of the blockchain can select different consensus modules according to the requirements of DAPP. In addition to the basic consensus methods currently provided by the system (POW, POS, PBFT, IPFS, DPOS), it also supports custom writing new consensus methods. In addition, the speed of the sub-chain above the block is not limited by the public chain, it is independent, you can customize the block speed, 5 seconds, 10 seconds or minutes or even an hour is OK.

The advantages of doing this are:

1. The complexity of deploying sub-chains is greatly reduced. You can directly use

existing consensus methods or just need to write sub-chain consensus and execution modules.

2. The sub-chain can be deployed quickly and flexibly, and a certain number of nodes are selected from the plurality of node pools participating in the system, thereby eliminating the trouble of maintaining the consensus node.

3. The nodes of ordinary users can easily participate in the consensus and gain revenue to achieve a win-win situation.

Secondly, the flexibility of the cost, the sub-chain can be deployed according to different application scenarios, when calling the function of the sub-chain, no more fees are charged, which greatly reduces the threshold for users to use DAPP, so that a large number of users can easily and quickly Use DAPP to experience the changes brought by blockchain technology, rather than the current blockchain application can only be limited to cryptocurrency enthusiasts.

Third, easy cross-chain, to achieve the Internet of Everything

The sub-chain function of the blockchain can implement cross-chain transactions between the main chain and other blockchains, for example, between Ethereum and Bitcoin; and, in a broader sense, implement blockchains and other The communication between the networks achieves the effect of the Internet of Everything.

Fourth, the sub-chain service provides powerful functions to build complex DAPP

The sub-chain can be used not only as a support platform for DAPP, but also as a

public service to provide specific services for other sub-chains or DAPPs. These services can be decentralized file storage, completely random random number generators, professional processing functions such as deep learning for AI services. Supported by a variety of sub-chain services, you can build a powerful DAPP, or decentralized cloud services. Such a revolutionary application model will incite the existing cloud operations, which will have far-reaching impact.

Chapter 2 Bitcoin

2.1 Bitcoin

Bitcoin is a consensus network that has led to a new payment system and a fully digital currency. It is the first decentralized peer-to-peer payment network that is controlled by its users without the need for a central authority or intermediary. From the user's point of view, Bitcoin is much like the cash of the Internet. Bitcoin can also be seen as the most outstanding bookkeeping system available today.

2.2 Bitcoin founder

Bitcoin is the first currency to realize the concept of "secret currency". In 1998, Wei Dai first explained the concept of "secret currency" on the cypherpunks mailing list, namely: a cryptographic principle to control the issuance and trading of currency, rather than relying on the new monetary form of the central authority. In 2009, Satoshi Nakamoto (Satoshi Nakamoto alias) published the first bitcoin specification and proof of concept on the cryptography mailing list. At the end of 2010, Nakamoto took the project and did not reveal much about his identity. Since

then, many developers have worked on Bitcoin projects, and the Bitcoin community has grown rapidly.

Nakamoto's anonymous identity often causes unfounded concerns, many of which are related to the misunderstanding of Bitcoin's open source features. Bitcoin's protocols and software are publicly available, and any developer around the world can view their code or develop their own modified Bitcoin software version. Like current developers, Nakamoto's influence is limited to the changes he has made that others have adopted. Therefore, Nakamoto does not control Bitcoin. Well, today, the identity issue of the inventor of Bitcoin may be the same as the identity of the paper inventor.

2.3 Bitcoin production principle

Starting from the nature of Bitcoin, the essence of Bitcoin is actually a special solution generated by a bunch of complex algorithms. The special solution refers to a group of equations that can get an infinite number of (in fact, bitcoin is a finite number) solution. And each special solution can solve the equation and is unique. In the analogy of the renminbi, bitcoin is the serial number of the renminbi. You know the serial number on a banknote and you own the banknote. The process of mining is to seek the special solution of this equation group through a huge amount of calculation. This equation group is designed to have only 21 million special solutions, so the upper limit of Bitcoin is 21 million.

2.4 Bitcoin Network

No one has a bitcoin network, just like no one has the technology behind email.

Bitcoin is controlled by all Bitcoin users around the world. Developers can improve the software, but they can't force changes to the rules of the Bitcoin protocol because all users are free to choose the software they want to use. In order to maintain compatibility with each other, all users also need to choose software that follows the same rules. Bitcoin can only work properly if all users reach a consensus. Therefore, all users and developers are very motivated to accept and protect this consensus.

2.5 Bitcoin operation

From the user's point of view, Bitcoin is a mobile phone application or computer program that provides a personal bitcoin wallet that users can use to pay for and receive bitcoin. This is how Bitcoin works for most users.

Behind the scenes, the entire Bitcoin network shares a common ledger called a "blockchain." This general ledger contains every transaction processed so that the user's computer can verify the validity of each transaction. The authenticity of each transaction is protected by the electronic signature corresponding to the sending address, which gives the user full control over the bitcoin that is transferred from their own bitcoin address. In addition, anyone can take advantage of the computing power of specialized hardware to process transactions and receive Bitcoin rewards for this purpose. This service is often referred to as "mining."

2.6 Bitcoin advantage

Freedom of payment – you can pay and receive any amount of money instantly, whenever and wherever you want. No bank holidays, no borders, no

restrictions. Bitcoin allows its users to have full control over their funds.

Very low cost - there is currently no processing fee for the processing of bitcoin payments or very little handling fee. Users can include the handling fee in the transaction to get processing priority and receive confirmation of the transaction sent by the network faster. In addition, there are also merchant processors that assist merchants in processing transactions, converting bitcoins into fiat money every day and depositing the funds directly into the merchant's bank account. Because these services are based on Bitcoin, they can provide far less fees than PayPal or credit card networks.

Reduce the risk of merchants - Bitcoin transactions are safe, irrevocable, and do not contain sensitive or personal information from customers. This avoids the loss to the merchant due to fraud or fraudulent returns, and there is no need to comply with the PCI standard. In places where credit cards are unusable or fraud rates are unacceptably high, merchants can easily expand into new markets. The end result is lower costs, a larger market, and less administrative costs.

Security and Control - Bitcoin users have complete control over their transactions; it is not possible for merchants to charge fees that may or may not be found in other payment methods. Paying in Bitcoin eliminates the need to bind personal information to the transaction, which provides great protection against identity theft. Bitcoin users can also protect their funds through backup and encryption.

Transparency and Neutral – All information about Bitcoin's funding supply

itself is stored in the blockchain and can be verified and used by anyone in real time. No individual or organization can control or manipulate the Bitcoin protocol because it is password protected. This makes the Bitcoin core believed to be completely neutral, transparent and predictable.

2.7 block chain fork

Bitcoin forks, exactly what should be called a blockchain fork.

How is the blockchain fork generated?

This starts with the design of the blockchain itself. In the world of Bitcoin, it is a one-off transaction. The so-called transaction is the event that I transferred a bitcoin to you, and the block in the blockchain is the storage space used to record these transaction information. Bitcoin is every Ten minutes to create a block, the current block size is 1M, assuming that each transaction requires about 1KB, then 1M can accommodate up to 1024 / 1 = 1024 transactions, then only 1.7 transactions per second. Imagine if Alipay, which is currently used by billions of people, can only accept 2 transactions per second, can it still meet the demand?

Soft fork and hard fork

So bitcoin is fixed and must be 1M in size?

The answer is no, Bitcoin's original block size is 32M. Nakamoto does not intend to limit the block size. It is only used by a small number of people. Each block is only a few kilobytes in size. In order to avoid wasting computing resources, To avoid DDOS attacks to ensure the safe operation of the Bitcoin system, Nakamoto has temporarily limited the block size to 1M. In terms of the bitcoin transaction volume

at the time, this 1MB is sufficient and more than enough.

But now that nearly a decade has passed, people who use Bitcoin are becoming more and more acquainted. The size of 1M block poses a serious problem. Now due to the limitation of Bitcoin block size, the backlog of Bitcoin network has been overwhelmed. More transactions make the transaction confirmation very slow. In the slowest case, you transfer a bitcoin to your friend. He may receive your transfer after three days. At this time, you either wait or pay higher. The transaction fee, of course, even if you pay a higher transaction fee, you still have to wait.

In order to solve the above problems, everyone decided to expand the block, and then there are two slightly conflicting methods.

This is called the fork: soft fork and hard fork.

Chapter III Monero

3.1 About Monero

Monero was launched in April 2014. This is a fair, pre-announced release of the CryptoNote reference code. There are no premine or instamine, and there is no part of the block reward for development. The founder, thanks for the controversial changes that have been raised by some communities. As a result, the Monero core team abandoned the project with the community after this new core team. Since then, this core team has provided supervision. Since the launch, Monero has made several major improvements. Migrating blockchains to different database structures provides greater efficiency and flexibility, sets the minimum ring

signature size so that all transactions are private, and implements RingCT to hide the amount of transactions. Almost all improvements have improved security or privacy, or promoted use. Monero continues to evolve with privacy and security goals in mind, ease of use and efficiency.

3.2 The value of Monero

1. Security - Users must be able to trust Monero and their trading information without risk of errors or attacks. Monero gave the miners full compensation, they are the most important members of the network, they provide security. With the latest and most flexible encryption tools, transactions are encrypted and secure.

2. Privacy - Monero values privacy. Monero needs to be able to protect users in court and, in extreme cases, protect users from it. This level of privacy must be completely open to all users, whether they have technical skills or not know how Monero works. A user needs to trust Monero with confidence so that he is not forced to change their spending habits because of the risks others have discovered.

3. Decentralization – Monero is committed to providing maximum decentralization. With Monero, you don't have to trust anyone on the network or run any large teams. An accessible "work proof" algorithm makes Monero on a regular computer easy, making it more difficult to purchase large amounts of mining rights. Nodes are connected to each other through I2P to reduce the risk of leaking sensitive transaction information and review (tba). Development decisions are very clear and open to discussion. The developer meeting log is posted online and is visible to everyone.

3.3 The difference between Monero and Bitcoin

Monero is not based on bitcoin.

It is based on the CryptoNote protocol. Bitcoin is a completely transparent system, and people can see exactly how much money is sent from one user to another. Monero hides this information to protect the privacy of users in all transactions. It also has several other variations such as dynamic block size and dynamic cost, proof of anti-ASIC work and tail coin emissions.

3.4 Monero development route

2014

[2014-04-18]: Launched Bitcointalk

[2014-04-23]: Renamed Monero from Bitmonero

[2014-09-04]: Recover from spam attacks

[2014-09-12]: Monero Research Lab Papers 1 and 2 Publishing

[2014-09-25]: Published Monero Research Lab Paper 3

[2014-12-08]: Release of version 0.8.8.6

2015

[2015-01-26]: Published Monero Research Lab Paper 4

2016

[2016-01-01]: 0.9.0 Hydrogen Helix released

[2016-02-10]: Published Monero Research Lab Paper 5

[2016-03-22]: In all transactions, the minimum number of laps required for hard forks is 3.

[2016-09-18]: 0.10.0 Wolfram Warptangent released

[2016-09-21]: Separate coins and coins with hard forks.

[2016-12-14]: 0.10.1 Wolfram Warptangent released

[2016-12-22]: Official GUI Beta 1 release

2017

[2017-01-05]: Hard fork enabled RingCT transaction

[2017-02-22]: Released at 0.10.2; serious bug fixes

[2017-03-27]: 0.10.3.1 released Wolfram Warptangent

[2017-04-15]: Try to adjust the minimum block size and dynamic cost algorithm

[2017-07-04]: Website release

[2017-09-07]: 0.11.0.0 Helium Hydra released

[2017-09-07]: Fragment blocks (Fluffy blocks)

[2017-09-10]: GUI exits beta

[2017-09-15]: Hard forks increase the minimum ringsize to 5 and require RingCT transactions.

[2017-09]: 0MQ/ZeroMQ

undone:

Scuffy blocks

GUI porting to Android

Redesigning the forum funding system

Secondary address

Multi-signature (multi-signature)

Kovri alpha released

future

Other MRL research papers

A second layer solution that provides speed and scalability

More effective range proves that RingCT reduces transaction size

Chapter IV INSO Capital

4.1 About INSO Capital

Aberdeen plc is one of the world's largest investment companies. Consolidated in 2017 by Standard Life plc and Aberdeen Asset Management PLC. Operating under the INSO Capital brand. Make it the UK's largest active manager and one of the largest active managers in Europe with significant global influence and scale and expertise to help clients achieve their investment goals.

4.2 MKcoin

MKcoin, an open source blockchain project incubated by INSO Capital, is a sub-chain technology built on Monero's CryptoNote protocol. MKcoin effectively inherits the privacy, decentralization and scalability attributes of the main chain Monero. Its powerful scalability eases the storage pressure of the main chain. With its customized DPOS consensus mechanism, it can meet more commercial applications such as DAPP in the future. The need for its custom execution module enhances the speed of the block and provides a smoother trading system. The

project was launched in June 2019. A total of 8,000 million pieces were issued. A block is a container for transactions, adding a new block to the blockchain every 2 minutes (see the constant DIFFICULTY_TARGET_V2 defined as 120 seconds). The block also contains a special type of transaction, the coinbase transaction, which adds the newly created MKcoin to the network. The block is created by the mining process, and the nodes of the block are successfully mined and then broadcast to each node connected to it, which then rebroadcasts the block until the entire MKcoin network has received the block. It is often impossible to create fake or bad blocks because the nodes that receive the block always validate the transactions they contain based on a set of consensus rules that all nodes adhere to, including verifying the cryptographic signature on each transaction.

4.3 About MKcoin

MKcoin differs from Bitcoin and other cryptocurrencies in that transactions in the MKcoin blockchain do not show where money is coming from or going, providing anonymity and making the currency completely interchangeable. In addition, the amount of all transactions is hidden by ringCT, which is a feature of the Union Coin. For auditing or other transparent purposes, users can share view keys to prove that they control a certain number of MKcoins.

MKcoin is the leading cryptocurrency, focusing on private and censorship transactions.

Most existing cryptocurrencies, including Bitcoin and Ethereum, have transparent blockchains, which means transactions are publicly verifiable and can be tracked by

anyone in the world. In addition, the addresses that send and receive these transactions may be linked to the true identity of a person.

MKcoin uses encryption to block the sending and receiving addresses and the transaction amount. MKcoin transactions are confidential and cannot be tracked. By default, each MKcoin transaction confuses the send and receive addresses and the transaction amount. This always-on privacy means that every MKcoin user's activity will enhance the privacy of all other users, unlike alternative transparent cryptocurrencies such as Zcash.

MKcoin is an alternative. By confusing, MKcoin will not be polluted by participation in previous transactions. This means that MKcoin will always be accepted without the risk of being reviewed.

The Kovri project currently under development will route and encrypt transactions through the I2P Invisible Internet Project node. This will obscure the trader's IP address and provide further network monitoring protection.

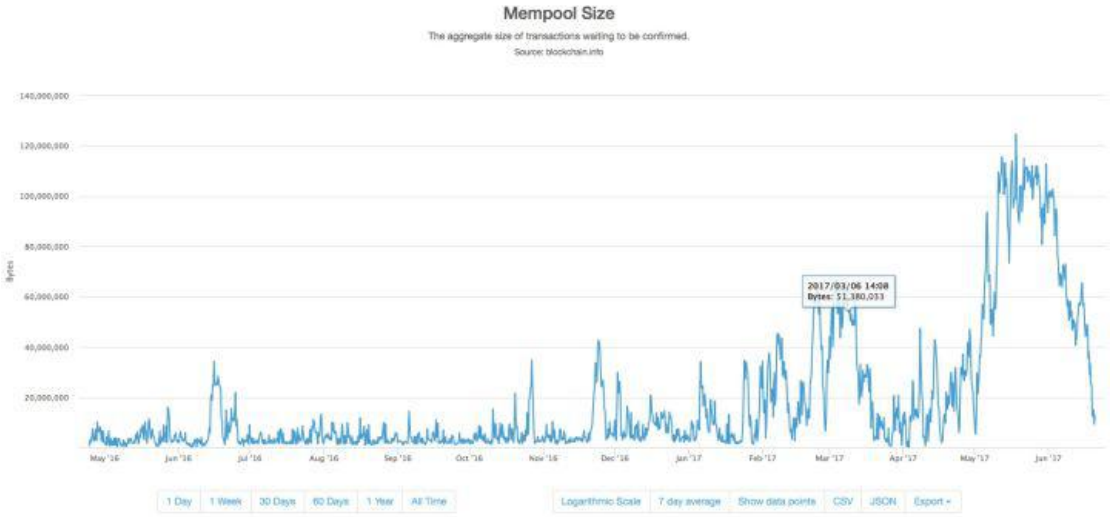
MKcoin is a grassroots community that attracts the world's best cryptocurrency researchers and engineering talent.

More than 500 developers contributed to the Coin project, including 30 core developers. Forum and chat channels are hospitable.

MKcoin's research labs, core development teams and community developers are constantly pushing the frontiers of cryptocurrency privacy and security.

MKcoin is an electronic cash payment that can be paid quickly and cheaply around the world.

There are no multi-day holding periods and there is no risk of fraudulent refunds. It is not subject to "capital control" – these are measures that limit traditional currency flows in countries with economic instability, sometimes even extremes.



4.4MKcoin blockchain expansion

The blocking problem of the transaction pool has been very serious recently, and it will only be more serious as users increase. The result of a large number of transactions not written into the chain is the increase in transaction fees - because each transaction is given to the miner how much transaction fee, and the miner will naturally choose the high transaction package for the transaction fee, then the situation will be low transaction costs The transaction is always stuck in the queue.

The significance of the expansion of the Union Coin, in addition to solving the problem of transaction congestion, increase the speed of transactions, the price of the currency rose. It will also drive the promotion of Internet popularity and development. The increase in blockchain capacity will also drive the popularity and development of blockchains.

4.5 Differences between MKcoin and other currencies

Non-traceable transaction

In this section, we propose a completely anonymous transaction scheme that satisfies substandard and unrelated conditions. An important feature of our solution is its autonomy: the sender does not need to work with other users or trusted third parties to conduct transactions; therefore each participant independently generates coverage traffic.

1, literature review

Our solution relies on the encryption primitives that become group signatures. First proposed by D. Chaum and E. van Heyst [19], which allows the user to sign his message on behalf of the group. After the user signs the message (for verification purposes) it is not his own single public message 1 This is called the "soft limit" - the reference customer limit for creating new blocks. The maximum hardness possible blockize is 1 MB key, but the key to all his users. The verifier believes that the true signer is a member of the group, but does not specifically identify the signer. The original agreement requires a reliable third party (called a group manager), who is the only one that can track the signer. The next version introduced by Rivest et al. is called a ring signature. In [34], there is an autonomous plan with no group manager and anonymous withdrawal. Various modifications to the scheme appear later: the linkable ring signature [26, 27, 17] allows to determine whether two signatures are generated by the same group of members, traceable ring signatures [24, 23] by providing the possibility to track the signer To limit excessively anonymous two messages about the same meta-information (or [tag]

of [24]). A similar cryptographic structure is also known as an ad hoc group signature [16, 38]. It emphasizes any combination, while the group/ring signature scheme means a fixed set of members. In most cases, our solution is based on E. Fujisaki and K. Suzuki's "Remoteable Ring Signature" [24]. To distinguish between the original algorithm and our modifications, we refer to the latter as a one-time ring signature, emphasizing the ability of the user to generate only one valid signature under its private key. We weaken traceability and maintain linkability, providing consistency only: public keys may appear in many foreign verification sets, and private keys can be used to generate unique anonymous signatures. If the double cost is tried, the two signatures will be linked together, but for our purposes, revealing the signer is unnecessary.

2, the definition

2, 1 Elliptic curve parameters As our basic signature algorithm, we chose to use the fast scheme EdDSA developed and implemented by D.J. Bernstein et al. [18]. Like Bitcoin's ECDSA, it is based on the elliptic curve discrete logarithm problem, so our solution can be applied to Bitcoin in the future. Common parameters are: q: prime number; q = 2255 - 19; d: element of Fq; d = -121665/121666; E: elliptic curve equation; -x2 + y2 = 1 + dx2y2; tt: a base point tt = (x , -4/5); l: the main order of the base points; l = 2252 + 27742317777372353535851937790883648493; Hs: cryptographic hash function {0,1} *→Fq; Hp: deterministic hash function E(Fq)→ E(Fq). 4.2.2 Terminology Enhanced privacy requires a new term that should not be

confused with Bitcoin entities. Private key ec-key: is a standard elliptic curve private key: aaa∈[1,l - 1]; public ec-key: is a standard elliptic curve public key: point A = att; one-time keyword: yes A pair of private and public electronic keys; private user key: a pair of two different private keys (a, b); tracking key: is a private and public key pair (a, B) (where B = Btt and af = b); public user key: is a pair of two public ec keys derived from (a, b) (A, B); standard address: is given a humanized string with error correction Representation of the public user key; truncated address: is a representation of the second half of the public user key (point B) giving the humanized string with the error correction. The transaction structure is similar to the Bitcoin structure: each user can select several separate receipts (transaction output) and sign with the corresponding private key and send it to a different destination. In contrast to the Bitcoin model, the user has a unique private and public key. In the proposed model, the sender generates a one-time public key based on the recipient's address and some random data. In this sense, the incoming transaction of the same recipient is sent to the one-time public key (instead of directly to the unique address), and only the recipient can restore the corresponding private part to redeem his funds (using his unique Private key). Recipients can use the ring signature to pay for the funds, keeping their ownership and actual expenses anonymous. The details of the agreement will be explained in the next section.

3. Unable to pay

Once a classic Bitcoin address is published, it becomes an explicit identifier for

revenue payments, linking them together and binding to the recipient's pseudonym. If someone wants to receive an "unconstrained" transaction, he should communicate his address to the sender through a private channel. If he wants to receive a different transaction that cannot be proven to belong to the same owner, he should generate all the different addresses instead of his own pseudonym.

We propose a solution that allows users to post a single address and receive unconditional unlinkable payments. The destination of each CryptoNote output (by default) is a public key derived from the recipient's address and the sender's random data. The main advantage of Bitcoin is that by default each target key is unique (unless the sender uses the same data for each transaction to the same recipient). Therefore, there is no such problem as "address reuse" by design, and no observer can determine if any transaction is sent to a specific address or link two addresses together.

First, the sender performs a Diffie-Hellman exchange, getting the shared key from half of his data and recipient address. He then uses the shared key and the lower half of the address to calculate the one-time destination key. Recipients from these two steps require two different ec keys, so the standard CryptoNote address is twice the address of the Bitcoin wallet. The receiver also performs a Diffie-Hellman exchange to recover the corresponding secret key. The standard transaction sequence is as follows:

Alice wants to send a payment to Bob who has posted his standard address. She opens the address and gets Bob's public key (A, B). Alice generates a random r∈

[1,1 - 1] and computes a one-time public key P = Hs(rA)tt+B. Alice uses P as the destination key for the output, and the value R = rtt (as Diffie- Part of the Hellman exchange) is wrapped somewhere in the transaction.

Note that she can create additional output using a unique public key: the different recipient's keys (Ai, Bi) mean different Pis, even if the same r is used. Alice sends the deal. Bob checks the transaction for each process with his private key (a, b) and calculates P r = Hs(aR)tt + B. If Alice and Bob are the recipients of the transaction, then aR = artt = rA and P r = P. Bob can recover the corresponding one-time private key: x = Hs(aR)+ b, so P = xtt. He can spend this output at any time by signing a deal with x. As a result, Bob received a payment related to the one-time public key that could not connect to the viewer. Some additional notes: When Bob "recognizes" his transaction (see step 5), he actually uses only half of his private information: (a, B). This pair, also known as the tracking key, can be passed to a third party (Carol). Bob can entrust her with processing new transactions. Bob does not need to explicitly trust Carol because she cannot recover the one-time secret key p without Bob's full private key (a, b). This method is very useful when Bob lacks bandwidth or computing power (smartphone, hardware wallet, etc.).

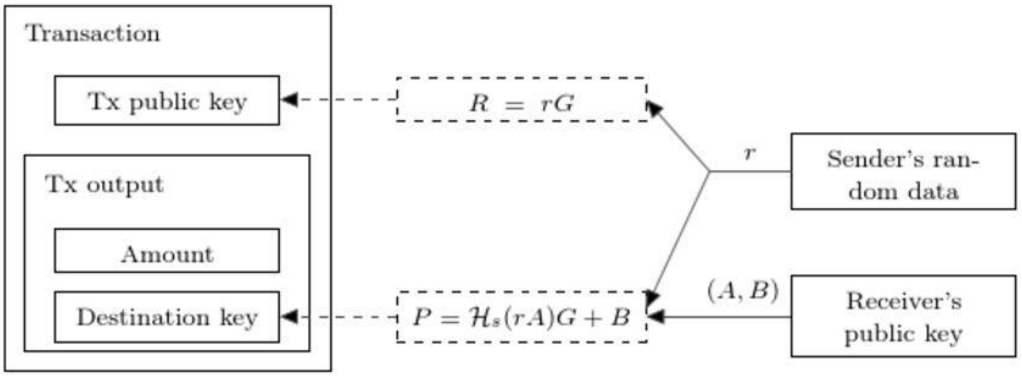


Fig. 4. Standard transaction structure.

If Alice wants to prove that she sent a transaction to Bob's address, she can disclose r or use any kind of zero-knowledge agreement to prove that she knows r (for example by signing a deal with r). If Bob wants to have an audit-compatible address that all incoming transactions can link to, he can post his tracking key or use a truncated address. This address represents only one public key B, and the rest of the protocol requirements are as follows: a = Hs(B) and A = Hs(B)tt. In both cases, everyone is able to "recognize" all Bob entry transactions, but of course, there is no money that can be spent without the secret key b.

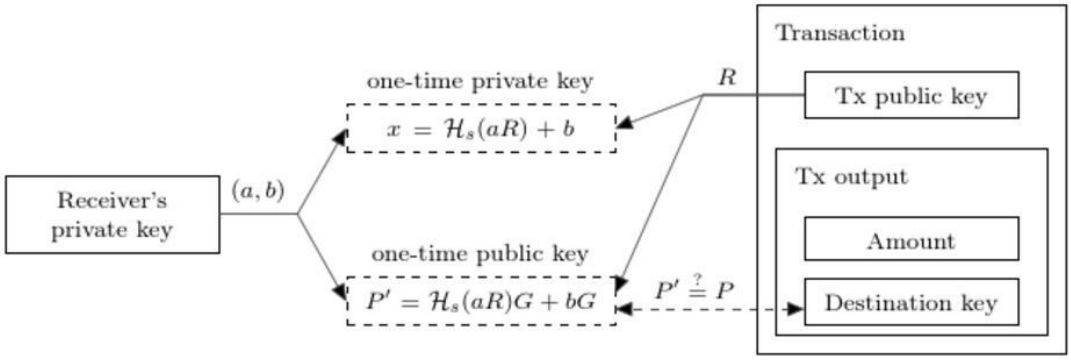


Fig. 5. Incoming transaction check.

4, one-time ring signature

A one-time ring signature based protocol allows the user to achieve unconditional connectionlessness. Unfortunately, common types of cryptographic signatures allow tracking of their respective sender and receiver transactions. We address this shortcoming in using different signature types than those currently used in electronic cash systems. We will first provide a general description of our algorithm without explicitly mentioning e-cash. The one-time ring signature contains four algorithms: (GEN, SIG, VER, LNK): GEN: takes public parameters and outputs ec pairs (P, x) and public keys I. SIG: Get message m, public key Sr Pi, if = s, a pair (Ps, xs), and output the signature σ and a set of S = Sr ∪ {Ps}. VER: Cancel message m, set S, signature σ , and output "true" or "false".

Compute

$$L_j = \alpha G$$

$$R_j = \alpha H_p(P_j)$$

$$c_{j+1} = h(\mathfrak{m}, L_j, R_j)$$

where h is a hash function returning a value in $\mathbb{Z}_q$. Now, working successively in j modulo n, define

$$L_{j+1} = s_{j+1}G + c_{j+1}P_{j+1}$$

$$R_{j+1} = s_{j+1}H_p(P_{j+1}) + c_{j+1} \cdot I$$

$$c_{j+2} = h(\mathfrak{m},\ L_{j+1},\ R_{j+1})$$

$$\ldots$$

$$L_{j-1} = s_{j-1}G + c_{j-1}P_{j-1}$$

$$R_{j-1} = s_{j-1}H_p(P_{j-1}) + c_{j-1} \cdot I$$

$$c_j = h(\mathfrak{m}, L_{j-1},\ R_{j-1})$$

LNK: Take the set I = {Ii}, sign σ and output "link" or "independent". The idea behind the protocol is quite simple: the user generates a signature that can be checked by a set of public keys instead of a unique public key. The identity of the signer is indistinguishable from the user in which the public key is in it until the owner generates the second signature using the same keyword.

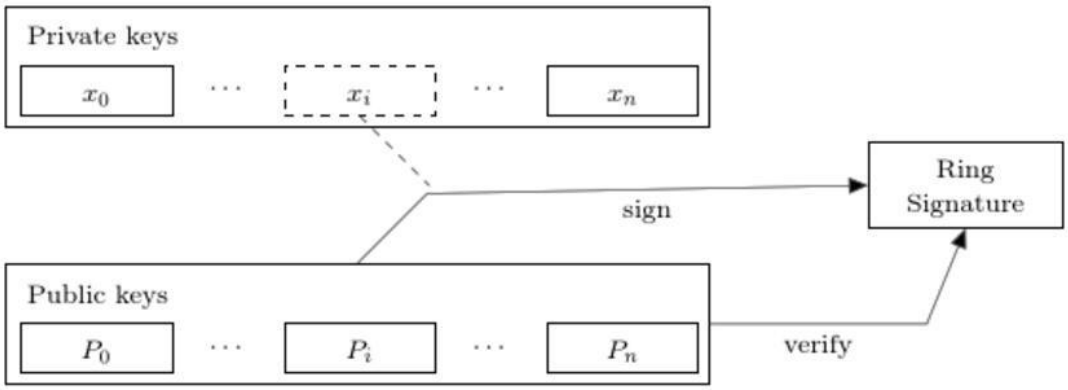


Fig. 6. Ring signature anonymity.

GEN: The signer chooses the random key x ∈ [1,1 - 1] and calculates the corresponding public key P = xtt. In addition, he calculates another public key I = xHp(P), which we call a "key image." SIG: The signer uses the technique in [21] to generate a one-time ring signature with non-interactive zero-knowledge proof. He selects a random subset of n from the public key Pi of his other user, his own key pair (x, P) and the key image I. Let 0 ≤ s ≤ n be the secret index of the signer in S (Make his public key Ps). He chooses a random {qi | i =0. . . n} and {wi | i = 0. . . n,i ƒ= s} from (1.l) and apply the following transformation: Li = Ri = .qitt, if i = s qitt + wiPi, if i ƒ = s if i = s qiHp(Pi) + wiI, then if =s The next step is to get a non-interactive challenge: c = Hs(m,L1,...,Ln,R1,...,Rn) Finally, the signer calculates

the response: wi, if I ƒ = s ci = n Ri = c - . Ci mod l, if i = si= 0 If I ƒ = s qs - csx mod l, if i = s the signature is σ =(I,c1,...,cn,r1,...,rn) .

$$L_\pi^j = \alpha_j G$$

$$R_\pi^j = \alpha_j H\left(P_\pi^j\right)$$

for random scalars α_j and $j = 1, ..., m$. Now, again analogously to section 2.1, set:

$$c_{\pi+1} = H\left(\mathtt{m}, L_\pi^1, R_\pi^1, ..., L_\pi^m, R_\pi^m\right).$$

$$L_{\pi+1}^j = s_{\pi+1}^j G + c_{\pi+1} P_{\pi+1}^j$$

$$R_{\pi+1}^j = s_{\pi+1}^j H\left(P_{\pi+1}^j\right) + c_{\pi+1} I_j$$

and repeat this, incrementing i modulo n until we arrive at

$$L_{\pi-1}^j = s_{i-1}^j G + c_{i-1} P_{i-1}^j$$

$$R_{\pi-1}^j = s_{i-1}^j H\left(P_{i-1}^j\right) + c_{i-1} \cdot I_j$$

$$c_\pi = H\left(\mathtt{m}, L_{\pi-1}^1, R_{\pi-1}^1, ..., L_{\pi-1}^m, R_{\pi-1}^m\right).$$

VER: The verifier checks the signature by applying an inverse transform: i = ritt + ciPi Ri = riHp(Pi)+ ciI N + Finally, the verifier checks if. Ci = Hs(m,Lr,...,Lr,Rr,...,Rr)mod l I = 0 0 N 0 N If this equality is correct, the verifier runs the algorithm LNK. Otherwise the verifier refuses to sign.

LNK: The certifier checks if I am using it in past signatures (these values are stored in set I). Multiple uses means that two signatures are generated under the same key. The meaning of the agreement: By applying the L conversion, the signer proves that he knows that x has at least one Pi = xtt. To make this proof non-repeatable, we introduce the key image as I = xHp(P). The signer uses the same coefficient (ri, ci) to prove the almost identical statement: he knows that x has at least one Hp(Pi) = I • x-1. If the mapping x→I is an injection: no one can recover the public key from the key image and identify the signer; the signer cannot use two different signatures for me and the same x. Appendix A provides a complete security analysis.

5, standard CryptoNote transaction

By combining two methods (unlinkable public key and untrackable ring signature), Bob reached a new level of privacy compared to the original bitcoin solution. It requires him to store only one private key (a, b) and publish (A, B) to begin receiving and sending anonymous transactions. In verifying each transaction, Bob only executes two elliptic curve polynomials, one at a time, to check if a thing belongs to him. For each of his outputs, Bob will restore the one-time keyword (pi, Pi) and store it in his wallet. Any input can be proven to have the same owner only when they appear in a single transaction. In fact, this relationship is difficult to establish due to a one-time signature. With a circular signature, Bob can effectively hide every input from others; all possible consumers will be equal, even if the previous owner (Alice) does not have any observer information. When signing his trade, Bob specified the same amount of external output as his output, mixing all the outputs without the involvement of other users. Bob himself (and others) don't know if any of these payments have already been spent: the output can be used as an ambiguity factor in thousands of signatures, not as a hidden target. A double expense check occurs during the LNK phase when checking the set of key images used. Bob can choose the ambiguity himself: n = 1 means that the probability he spends is 50%, and n = 99 gives 1%. The size of the resulting signature increases linearly with O(n + 1), so the anonymity of Bob's extra transaction costs is increased. He can also set n = 0 and have his ring signature contain only one element, but this will immediately show him as a cost.

4.6, MKcoin workload proof

We propose and study a new work verification algorithm. Our main goal is to reduce the gap between CPU (most) and GPU / FPGA / ASIC (minority) miners. It is appropriate for some users to have certain advantages over other users, but their investment should grow as power increases linearly. More broadly, production-specific equipment must be profitable as little as possible.

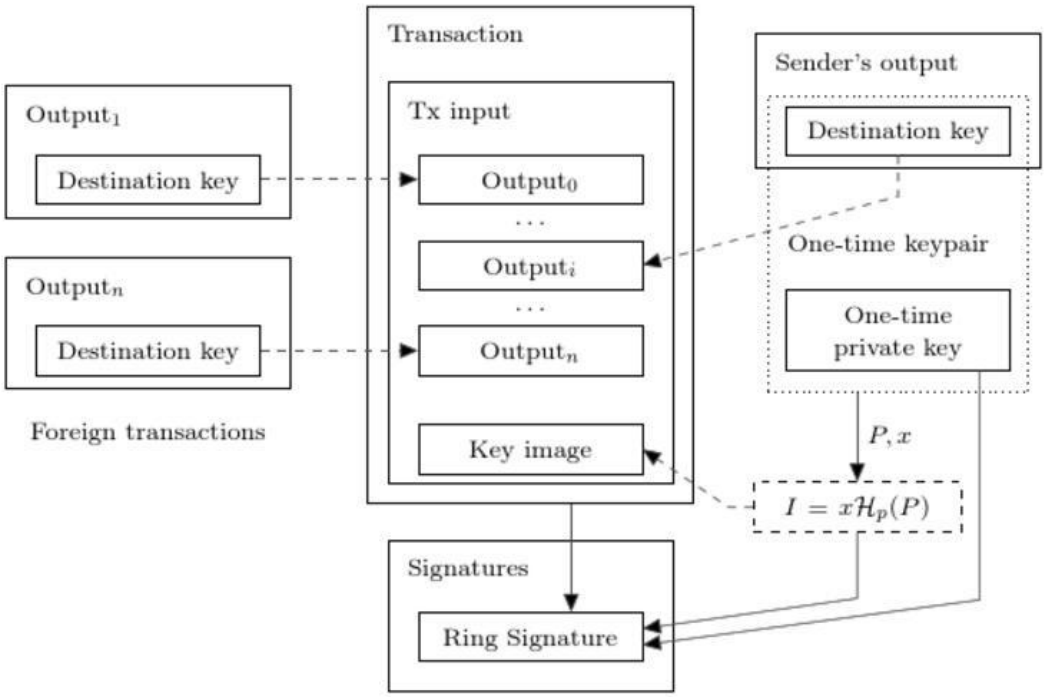


Fig. 7. Ring signature generation in a standard transaction.

4.6.1 Related work

The original Bitcoin work protocol uses the CPU-intensive pricing feature SHA-256. It consists primarily of basic logical operators and relies only on the computational speed of the processor, so it is perfectly suited for multicore/transmitter implementations. However, modern computers are not limited by the number of operations per second and are not limited by the size of the memory. Although some processors can be much faster than other processors [8], the memory size is less likely to change between machines. The memory limit function was first

introduced by Abadi et al. and was defined as the function of "calculation time is dominated by the time spent accessing memory" [15]. The main idea is to build an algorithm that allocates a large amount of data ("scratchpad") in memory that can be accessed relatively slowly (such as RAM) and "access unpredictable sequence of locations." A block should be large enough to preserve data more than recalculate for each access. The algorithm should also prevent internal parallelism, so N concurrent threads should require N times more memory at a time. Dwork et al. [22] investigated and formalized this approach, leading them to propose another variant of pricing: "Mbound." Another work belongs to F. Coelho [20], who proposed the most effective solution: "Hokkaido". According to our knowledge, the last work based on the idea of pseudo-random search in large arrays is the algorithm called "scrypt" by C. Percival [32]. Unlike previous features, it focuses on key derivations rather than work proof systems. Despite this fact, scrypt can serve our purposes: it performs well in partial hash conversion problems (such as SHA-256 in Bitcoin). Scrypt has now been applied to Litecoin [14] and other Bitcoin forks. However, its implementation is not a true memory limitation: the ratio "memory access time/total time" is not large enough because each instance uses only 128 KB. This will allow GPU miners to be approximately 10 times more efficient and continue to leave the possibility of creating relatively inexpensive but efficient mining equipment. In addition, the scrypt construct itself allows for a linear trade-off between memory size and CPU speed, due to the fact that each block in the scratchpad is only from the previous block. For example, you can store every

other block and recalculate other blocks in a lazy way, only if it becomes necessary. The pseudo-random index is assumed to be uniformly distributed, so the expected value of the additional block recalculation is 1 · N, where N is the number of iterations. The overall calculation time is increased by less than half because there are also time-independent (constant time) operations, such as preparing the scratchpad and hashing each iteration to save 2/3 of the memory cost. 1·N + 1·2·N = N additional Recalculation; 3 3 9/10 results in 1·N +. . . + 1·9·N = 4.5N. It's easy to show that only one of all blocks is stored for 10 10 seconds and the time is less than the s-1 factor. This in turn means that a machine with a CPU can store only 320 bytes of registers more than 200 times faster than modern chips.

4.6.2 Proposed algorithm

We propose a new memory limit algorithm for work pricing functions. It relies on random access to slow memory and emphasizes latency dependencies. Compared to each new block (64 bytes in length), it depends on all previous blocks. Therefore, the hypothetical "memory protection" should increase his calculation speed exponentially. Our algorithm requires approximately 2 Mb per instance for the following reasons: It applies to the L3 cache of modern processors (per core) and should become mainstream in the next few years; one megabyte of internal memory is almost unacceptable for modern ASIC pipes. Size; The GPU may run hundreds of concurrent instances, but is otherwise limited: GDDR5 memory is slower than CPU L3 cache, and its bandwidth is significant, not random access speed. A significant extension of the scratchpad will require an increase in the

number of iterations, which in turn means an increase in overall time. A "heavy" call in an untrusted p2p network can cause serious vulnerabilities because the node is obliged to check the proof of work for each new block. If a node spends a considerable amount of time in each hash evaluation, DDoS can be easily passed through a large number of fake objects with arbitrary working data (random numbers).

4.7, more advantages

4.7.1 Smooth release

The upper limit of the total number of CryptoNote digital coins is: MSupply = 264-1 atomic units. This is simply a natural limitation based on implementation restrictions, not an instinct like "N coins should be enough for anyone." To ensure the smoothness of the emissions process, we use the following formula to earn a point reward: BaseReward = (MSupply - A)18, where A is the amount of coins previously generated.

4.7.2 Adjustable parameters

4.7.2.1 Difficulties

CryptoNote includes a positioning algorithm that changes the difficulty of each block. When the network hash value increases or decreases sharply, this reduces the system's response time and maintains a constant blocking rate. The original Bitcoin method calculates the relationship between the actual and target time spans between the previous 2016 blocks and uses them as the multiplier for the current difficulty. Obviously this is not suitable for fast recalculation (because inertia

is large) and causes oscillation. The general idea behind our algorithm is to generalize all the work done by the node to the time it takes. The workload is the corresponding difficulty value in each block. But due to inaccurate and untrusted timestamps, we are unable to determine the exact time interval between blocks. The user can transfer his timestamp to the future, and the next time interval may be less likely or even negative. There are probably very few such events, so we can sort the timestamps and truncate the outliers (ie 20%). The remaining values range from 80% of the time spent on the corresponding block.

4.7.2.2 Size restrictions

The user pays for the storage block and has the right to vote. Each miner handles the balance between balancing costs and profitability and sets his own "soft limits" to create blocks. In addition, the core rule of the largest block size is necessary to prevent the block chain from being flooded by spurious transactions, but the value should not be hard coded. Let MN be the median of the last N block sizes. Then the "limit" to accept the block size is 2·MN. It prevents the block from expanding, but still allows the limit to grow slowly over time if needed. The transaction size does not need to be explicitly limited. It is limited by the size of the block; if someone wants to create a huge transaction through hundreds of inputs/outputs (or the ambiguity of the ring signature is high), he can do this by paying enough. 6.2.3 Fine size fines Miners still have the ability to fill their own zero-fee transactions, up to a maximum of 2. Mb. Although only most miners are able to adjust the median value, there is one possibility to swell the blockchain and create additional loads on the

nodes. To prevent malicious participants from creating chunks, we introduce a penalty function: NewReward = BaseReward·. BLKSIZE0.2 MN - This rule applies only when BlkSize is greater than the minimum available block size (10kb, MN·110%). When the overall charge exceeds the fine, miners are allowed to create "usually large" blocks, even exceeding profits. But the cost is unlikely to increase twice, unlike the penalty value, so there will be a balance.

4.7.3 Transaction script

CryptoNote has a very simple scripting subsystem. The sender specifies an expression Φ= f(x1,x2,...,xn), where n is the number of destination public keys Pi n. Only five binary operators are supported: min, max, sum, mul, and cmp. When the recipient pays the payment, he generates 0 ≤ k ≤ n signatures and passes them to the transaction input. The verification process simply evaluates Φ with xi = 1 to check the valid signature of the public key Pi, xi = 0. If Φ > 0, the verifier accepts the certificate. Although simple, this approach covers all possible situations: multiple/threshold signatures. For the bitcoin-style "M-out-of-N" multi-signature (ie the receiver should provide a valid signature of at least 0 ≤ M ≤ N) Φ = x1 + x2 +. . +xN ≥ M (for the sake of clarity, we use general algebraic notation). Weighted threshold signatures (some keys may be more important than others) can be expressed as Φ= w1·x1 +w2·x2 +. . . + wN·xN≥wM. And the primary key corresponds to a scene where Φ = max(M·x, x1 + x2 + ... + xN) ≥ M. It is easy to show that any complicated situation can be expressed by these operators, that is, they form the basis. password protection. Having the secret password s is

equivalent to the knowledge of the private key, deriving deterministically from the password: k = KDF(s). Therefore, the recipient can prove that he knows the password by providing another signature under the key k. The sender simply adds the corresponding public key to his output. Note that this method is more secure than the "transaction puzzle" used in Bitcoin [13]. Degraded cases. Φ = 1 means that anyone can spend money; Φ = 0 means that the output is never consumed. In the case where the output script is combined with the public key, it is too large for the sender, he can use a special output type, which means that the recipient puts the data in his input, and the sender only provides one Hash. This method is similar to Bitcoin's "pay-hash" feature, but instead of adding new script commands, we handle this at the data structure level.

4.8 bitcoin shortcomings and some solutions from MKcoin

4.8.1 Transaction traceability

Privacy and anonymity are the most important aspects of e-cash. Peer-to-peer payments are seen from a third-party perspective and are significantly different from traditional banking. In particular, T. Okamoto and K. Ohta describe six criteria for ideal electronic cash, including "Privacy: the relationship between the user and his purchase must be pursued by no one" [30]. From their description, we derive the attributes that must be met by two fully anonymous electronic cash models to meet the requirements outlined by Okamoto and T. Okamoto and K. Ohta Daejeon: Untrackability: For each incoming transaction All possible senders are equal in probability. No relevance: For any two external transactions, it is not possible to

prove that it is sent to the same person. Unfortunately, Bitcoin does not meet non-retroactivity requirements. Since all transactions that occur between network participants are public, any transaction can be explicitly traced back to unique origins and final recipients. Even if two participants exchange funds in an indirect way, an appropriately designed path finding method will reveal the origin and the ultimate recipient. Others suspect that Bitcoin does not meet the second property. Some researchers have indicated ([33, 35, 29, 31]) that careful blockchain analysis may reveal the link between Bitcoin network users and their transactions. Although there are some methods controversial [25], it is suspected that a lot of hidden personal information can be extracted from the public database. Bitcoin failed to meet the above two characteristics, leading us to conclude that it is not an anonymous, but a pseudo-anonymous electronic cash system. Users quickly develop solutions to circumvent this shortcoming. Two direct solutions are "money laundering services" [2] and the development of distributed methods [3, 4]. Both solutions are based on mixing several public transactions and sending their ideas through some intermediate address; this in turn has the disadvantage of requiring a reliable third party. Recently, Miers et al. proposed a more creative approach. [28]: "Zerocoin". Zerocoin utilizes an encrypted one-way accumulator and zero-knowledge proof, allowing users to "convert" bitcoin to zero contention and use anonymous proof of ownership instead of digital signatures based on public passwords. However, this knowledge proves to have a constant but inconvenient size - about 30kb (based on today's bitcoin limit), which makes the proposal

impractical. The author acknowledges that the agreement is unlikely to be accepted by most Bitcoin users [5].

4.8.2 Proof of workload

Bitcoin creator Satoshi Nakamoto described most decision algorithms as "one CPU, one vote" and used the CPU limit price pricing feature (double SHA-256) as its workload proof scheme. Since users vote for a single transaction history order [1], the rationality and consistency of this process is a key condition for the entire system. The security of this mode has two drawbacks. First, it requires 51% of the network mining power to be controlled by honest users. Second, the system's progress (bug fixes, security fixes, etc.) requires that most users support and agree to the changes (this happens when users update their wallet software) [6]. Finally, this same voting mechanism is also used for collective opinion polls to implement certain features [7]. This way we can speculate on the attributes that the job pricing function must satisfy. This feature does not give network participants a greater advantage than another participant; it requires a balance between the high cost of common hardware and custom devices. As you can see from the recent example [8], the SHA-256 feature used in the Bitcoin architecture does not have this feature because it is more efficient to capture on GPUs and ASIC devices than high-end CPUs. As a result, GPU and ASIC owners have greater voting power than CPU occupants, so Bitcoin creates a favorable gap between participants' voting power because it violates “one CPU, one vote” in principle. This is a typical example of the Pareto principle, where 20% of system participants control more than 80% of

the votes. One can argue that this inequality has nothing to do with the security of the network, because the number of participants who control most votes is small, but the honesty of these participants is important. However, such arguments have some drawbacks because they may be cheap professional hardware, not the honesty of the participants. To illustrate this, let's look at an example. Suppose a vicious individual acquires his own mining site by cheaply, gaining the enormous mining power of the previously described hardware. Assuming that the global hash value drops significantly, even for a while, he can now use his mining capabilities to branch and double spend. As we will see later in this article, the events described earlier are unlikely to happen.

4.8.3 Irregular release curve

Bitcoin has a predetermined emission rate: each resolved block produces a fixed amount of coins. About once every four years, this pay is halved. The original goal was to create a finite smooth emission with exponential decay, but in reality we have a piecewise linear launch function whose breakpoints can cause problems with the bitcoin infrastructure. When breakpoints occur, miners begin to receive only half of their previous pay. The absolute difference between BTC (expected in 2020) seems to be tolerable. However, when reviewing the 50 to 25 BTC declines that occurred on November 28, 2012, this was not appropriate for a large number of mining community members. Figure 1 shows the sharp drop in the network hash rate at the end of November, just in the halving. This incident may have been the perfect moment for a malicious individual to perform a double-spending attack as

described in the Work Function section [36].

4.8.4 Hard Coded Constants

Bitcoin has many hard-coded restrictions, some of which are natural elements of the original design (such as block frequency, maximum money supply, confirmed quantity), while others seem to be artificially constrained. This is not the limit, because it cannot be changed quickly. They cause major shortcomings if necessary. Unfortunately, it is difficult to predict when constants may need to change, and replacing them can have dire consequences. Hard-coded limit changes lead to catastrophic consequences

A good example of this is the block size limit set to 250kb1. This limit is sufficient to accommodate approximately 10,000 standard transactions. In early 2013, this limit was almost reached and an agreement was reached to increase the limit. This change was implemented in wallet version 0.8, ending 24 block splits and successful double cost attacks

[9]. Although the error is not in the Bitcoin protocol, but in the database engine, if there is no artificially introduced block size limit, it can easily be captured by a simple stress test. Constants are also the form of concentrated points. Despite the P2P equivalence of Bitcoin, most nodes use an official reference client developed by a small group of people.

[10]. The group decided to implement the changes to the agreement, and most people accepted the changes regardless of their "correctness."

Some decisions have sparked heated discussions and even called for boycotts [11], suggesting that communities and developers may disagree with certain important points. Therefore, protocols with user configurable and self-tuning variables seem logical as a possible way to avoid these problems.

4.8.5 huge script

Bitcoin's scripting system is a heavy and complex feature. It may allow for the creation of complex transactions [12], but due to security issues, some of its features are disabled and some are not even used [13]. Bitcoin's most popular trading scripts (both in the sender and receiver) look like this:

OP DUP OP HASH160 OP EQUALVERIFY OP CHECKSIG. The script is 164 bytes long and its sole purpose is to check if the recipient has the key needed to verify its signature.

4.9. Conclusion

We investigated the main pitfalls of Bitcoin and proposed some possible solutions. These advantages and our ongoing development have made the new electronic cash system CryptoNote a serious rival to Bitcoin, surpassing all forks. Nobel laureate Friedrich Hayek proved in his famous work that the existence of an independent currency has a huge positive effect. Every currency issuer (or developer in our case) is attracting users by improving his products. Money is like a

commodity: it can have unique interests and shortcomings, and the most convenient and trustworthy currency has the greatest demand. Suppose we have a comparative advantage currency: this means that Bitcoin will grow faster and become better. The biggest support for open source projects comes from users who are interested in it. We don't think CryptoNote is a complete replacement for Bitcoin. Conversely, having two (or more) powerful and convenient currencies is better than just one. Running two or more different projects in parallel is the natural flow of the electronic cash economy. Security We will give proof of our one-time signature plan. In a way, it is consistent with the part proved in [24], but we decided to rewrite them with reference instead of forcing the reader to go from one piece of paper to another. These are the attributes to be built: Linkability. Given all the secret keys {xi} i = 1 of the set S, it is impossible to generate n + 1 valid signatures σ1, σ2. . . , σn+ 1, so that they all pass the LNK phase (ie, have n + 1 different key images Ii). This attribute means double spending protection in the context of CryptoNote. Defensive ability. Given a set S, up to n-1 corresponding private keys xi (excluding i = j) and the image xj of the key xj are unlikely to produce a valid signature σ with Ij. This attribute means theft protection in the context of CryptoNote. Unforgeable. Given only one public key set S, it is impossible to generate a valid signature σ . Anonymity. Given the signature σ and the corresponding set S, it is not possible to determine the signer's secret index j with a probability p > 1. Connectivity

Theorem 1. Our one-time ring signature scheme is linked by a random oracle

model. prove. Suppose the opponent can generate n + 1 valid signatures σiii*f* = Ij with key images for any i,j∈[1]. Since #S = n, there is at least one Ii*f* = xiHp(Pi) for each i. Consider the corresponding signature σ = (I, c1, ..., cn, r1, ..., rn). VER(σ) = "true", which means Lr i = ritt + ciPiRr i = riHp(Pi) + ciI ñ . Ci = Hs(m,Lr,...,Lr,Rr,...,Rr)mod lI = 1 1 N 1Ñ The first two equality means I.logG Lr = ri + cixi log HP(PI) Rr = ri+ci log Hp(Pi)I where logA B informally represents the discrete logarithm of B to base A. As shown in [24], we note that $ i:xi = logHp(Pi)I means that all ci are uniquely determined. The third equality forces the opponent to find the previous image of Hs to successfully attack an event whose probability is considered negligible. Justifiable ability

Theorem 2. Our one-time ring signature scheme is negligible under the discrete logarithm assumption in the random oracle model. prove. Suppose the opponent can generate a valid signature σ=(I,c1,...,cn,r1,...,rn), where I = xj HP(Pj) is given {xi | i = 1, . . , j-1, j + 1,... . , n}. Then, we can construct an algorithm that solves the discrete logarithm problem in E(Fq). Assuming that inst = (tt, P) ∈ E(Fq) is a given instance of DLP, and the goal is to obtain s such that P = Stt. Using standard techniques (eg [24]), A simulates random and signed words and causes the opponent to generate two valid signatures of Pj = P in set S: σ=(I,c1,...,cn,r1,. .., rn) and σr = (I, cr, ..., cr, rr, ..., rr). 1n 1 n rj -rt Since I = xj Hp(Pj) in both signatures, we calculate xj = logHp(Pj)I = ct Maud A output xj because Lj = rjtt + cj Pj = rr tt + cr Pj And Pj = P.不可 Unforgeability

It has been shown in [24] that unforgeability is only one meaning of linkability and exclusion. Theorem 3. If the one-time ring signature scheme is linkable and can be cancelled, it is unforgeable. prove. Suppose an opponent can falsify the signature of a given set S: σ0=(I0,...). Consider all valid signatures (generated by honest signers) for the same message m and set S: σ1, σ2,. . . , σn. There are two possible scenarios: I0∈{Ii n. Which are illegal. I0ƒ∈{Ii n. Which contradicts the linkability. anonymous

Theorem 4. Our one-time ring signature scheme is anonymous under the decisive Diffie-Hellman assumption in the random oracle model. prove. Suppose the opponent can determine the signer's secret index j with a probability p = 1 + s. Then we can construct algorithm A, which solves the decisive Diffie-Hellman problem in E(Fq) with a probability of 1 + s. 2 2 Let inst =(tt1,tt2,Q1,Q2)∈E(Fq) be an instance of DDH and determine if logG1 Q1 = logG2 Q2. A is provided to the opponent with a valid signature σ0=(I,...), where Pj = xjtt1 = Q1 and I = Q2 and simulates oracle Hp, returning tt2 to query Hp(Pj). The opponent returns k as his guess for index i: I = xiHP(Pi). If k = j, A returns 1 (for "yes"), otherwise it is random r ∈{1,0}. The probability of correct selection is as shown in [24]: 1 + Pr(1 | inst∈ DDH)-Pr(1 | inst∈/ DDH)= 1 + Pr(k = j | inst∈DDH)+ 2 2 Pr(Kƒ = j | inst ∈DDH)·Pr(r = 1)-Pr(k = j | inst∈/ DDH)-Pr(kƒ = j | inst∈/ DDH) = 1 1 n-1 1 1 n-1 1 1 s 2 + n + s +(n - s)·2 - n - n·2 = 2 + 2 In fact, the result should be reduced by the probability of collisions in Hs, but this value is considered negligible . Regarding the annotation of

the hash function Hp we define Hp as a deterministic hash function E(Fq)→E(Fq). None of the proofs required Hp to be an ideal cryptographic hash function. The main purpose is to obtain a pseudo-random number of the image key I = xHp (xtt) in a certain certain way. Using a fixed base (I = xtt2), the following may be true: Alice sends two standard transactions to Bob, producing a one-time tx key: P2 = Hs(r1A)tt + B and P1 = Hs(r2A)tt+B Bob restores the corresponding private tx keys x1 and x2 and spends an output with a valid signature and image keys I1 = x1tt2 and I2 = x2tt2. Now, Alice can link these signatures and check the equation I1 -I2 = (Hs(r1A) - Hs(r2A)) tt2. The problem is that Alice knows the linear correlation between the public keys P1 and P2, and in the case of the fixed base tt2, she also obtains the same relationship between the key images I1 and I2. Replace tt2 with hp(xtt2), which does not retain linearity and fixes this flaw. To construct a deterministic Hp, we use the algorithm proposed in [37].

5.0, INSO Capital Fund Team

Paul Aggett•External Director

been a Director of the ying sheng Foundation since its creation as the ying sheng Foundation and I was involved in the debates around the original set up and structure. The most pleasing aspect to me is YSF provides additional goodwill and enhanced reputation for the organisation both internally and externally and has been seen as a positive to staff morale.

Along with YSF I have participated in the Global Volunteering Day. Last year I

attended FareShare in Bermondsey and was pleased to be told that Fareshare had started up in Ipswich close to my home. I have since spent a few days volunteering there thanks to the original company connection.

I have always been involved with at least one charity during my career and see this as a small way of giving something back to the community. I am also a Trustee Director of Freeword based in London.

Tamsin Balfour•Chairman

Whilst our corporate purpose is to help others invest for a better future, planning for that future is impossible for the many people who are worried about today. Helping people to achieve their potential has always driven me, both inside and outside the office, so I′ m delighted to have been given the privilege of helping to deliver our charitable giving in order to help others access that better future. I′ m also keen to encourage our people to get involved with the work of the foundation - for themselves, for us, and for our communities across the globe.

Bev Hendry•Director

I have worked in the investment management business for over 30 years and being able to give back to a society that has been especially good to me is certainly fulfilling. As a child, I was a beneficiary of a charitable scholarship which started me on my career path. As the YSF representative on the Board, I am honored to participate in charitable projects which significantly help those members of our

local communities who are in need of assistance.

Michael Tumilty•Director

I’ m delighted to be part of the Foundation Board here at YSF. Charitable giving affords us with a massive opportunity for all of us to make a difference to people who are not as fortunate as ourselves. Charitable giving creates a means by which we can make a sustainable difference to help people live better lives and that in itself is so rewarding. I sit on a number of Charity Boards and the work that the Charities do is humbling in so many different ways. Knowing that I can make just a small difference is what motivates me to contribute as best I can.

Lynn Warren•Director

Lynn Warren is Head of CEO Office at Standard Life Aberdeen plc, supporting the CEO with the delivery of both strategic and cultural goals.

Outside of work, Lynn has a strong interest in working with vulnerable groups – from supporting children through dance to caring for the elderly in her local community. Lynn has also supported local projects for charities including Marie Curie, Barnardos and CCLASP.

Lynn was delighted to be invited to join the Board of Aberdeen Standard Investments Charitable Foundation enabling her to support our company purpose through meaningful investments in our global communities.

Hugh Young•Director

I’m fortunate to be in a position to help those who haven’t been as lucky or as privileged as I have been. The thrust of our charitable efforts has been on the health and education of the young in the less developed world , a subject particularly dear to me heart as , in an indirect and diluted sense , it’s part of my day job - bringing in capital to emerging markets , assisting in raising living standards and improving work practices. Better health and education will enable many to enjoy the opportunities I’ve had.

5.1, MK coin team

The MKcoin Management Committee brings together the heads of the main investment areas within Blockchain. It comprises our senior investment staff, who are in overall charge of specific investment capabilities, operations (such as investment execution and governance) and asset classes.

Mandy Pike

Global Head of Investment Execution

Prior to that, Mandy was an Investment Dealer at F&C Investment Management. Before that, Mandy worked at BNP Capital Markets. Her City career began at Grieveson Grant in the private client department. Mandy has a wealth of experience and is widely recognised across the industry as one of the most experienced and insightful dealing practitioners.

Sean Phayre

Global Head of Quantitative Investing

Sean has been with Aberdeen since 2014, having joined as part of the SWIP transaction. Sean led the development and management of quantitative strategies and structured product capabilities in both Equities and Fixed Interest. He began his investment career at Edinburgh Fund Managers (EFM). He established quantitative investment teams at both EFM and SWIP.

Peter McKellar

Global Head of Private Markets

Peter heads the private equity, infrastructure, real assets, strategic credit and private markets solutions business of KKcoin; the business has £17bn of AUM. Peter is based in the Edinburgh and London offices, and joined Standard Life Investments in 1999. Starting his career in investment banking at JP Morgan in 1987 and working in corporate finance, Peter moved into industry in 1995 as Corporate Development Director and then Group Finance Director of Clydeport plc, a London listed company and former Montagu buyout. He has a LLB (Hons) degree in Law from The University of Edinburgh.

Robert McKillop

Global Head of Product and Client Solutions

Robert Joined Standard Life Investments as a Japanese portfolio manager in 1997 from Scottish Amicable Investment Managers. In 2002 he was promoted to the position of Head of Japanese Equities. In 2008 Robert moved to the Global Equities desk as Head of EAFE Funds. Following almost three years in that position Robert joined the Global Client Group management team in 2010 as Global Head of Product & Investment Specialists. In 2016 Robert was appointed to the SLI Global Operating Committee. In October 2018 he was appointed Global Head of Product & Proposition for MKcoin. His current role is Global Head of Product and Client Solutions.

Aymeric Forest

Global Head of Multi-Asset Investing

Aymeric joined ASI in February 2019 as Global Head of Multi-Asset Investing. Prior to that he had investment leadership roles within Multi-Asset Portfolio Solutions at Schroders for 7 years. He was Global Head of GIS at BBVA in 2009 and took various senior investment roles within Multi-Asset at ABN AMRO AM for 7 years. Aymeric has over 20 years of experience in Asset Management and has worked in Paris, Luxembourg, Madrid and London.

Archie Struthers

Global Head of Investment Governance and Oversight

Archie joined MKcapital in January 2017 as Head of Investments, having previously

been Global Head of Investment Solutions at Aberdeen Asset Management. Prior to this he was Managing Director of Investment Solutions at SWIP and Chief Operating Officer of Multi-Asset Client Solutions at Blackrock. He was appointed Global Head of Investment Governance & Oversight in August 2017.

Ginny Richardson

Head of CIO Office

Ginny joined ying sheng Capital in 2009 and has worked across the business in a variety of roles, predominantly focused on strategy and corporate development. In December 2016, she started in her current role as Head of CIO Office incorporating functional strategy, business management and communications. Prior to that, Ginny was Strategic Development Director for ying sheng Capital Investments.

Archie Struthers

Global Head of Investment Governance and Oversight

Brian joined ying sheng capital 2018, having started his career as a quantitative analyst. He previously held the position of Head of Multi-Asset Risk and Structuring managing several types of investment strategies, including liability driven investment (LDI) and absolute return. With the merger, Brian was appointed Global Head of Investment Innovation.

5.2MKcoin wallet interface example

This is a list of MKcoin-wallet-rpc calls, their inputs and outputs, and an example of each call. The program MKcoin-wallet-rpc replaces the rpc interface in simplewallet, followed by MKcoin-wallet-cli.

All MKcoin-wallet-rpc methods use the same JSON RPC interface. E.g:

```
IP=127.0.0.1
PORT=18082
METHOD="make_integrated_address"
PARAMS="{\"payment_id\":\"1234567890123456789012345678900012345678901
 234567890123456789000\"}"
curl \
   -X POST http://$IP:$PORT/json_rpc \
   -d
'{"jsonrpc":"2.0","id":"0","method":"'$METHOD'","params":'"$PARAMS"'}
' \
   -H 'Content-Type: application/json'
```

如果使用--rpc-login 参数 as 执行 monero-wallet-rpc username:password，请按照以下示例操作：

```
IP=127.0.0.1
PORT=18082
METHOD="make_integrated_address"
PARAMS="{\"payment_id\":\"1234567890123456789012345678900012345678901
 234567890123456789000\"}"
curl \
   -u username:password --digest \
   -X POST http://$IP:$PORT/json_rpc \
   -d
'{"jsonrpc":"2.0","id":"0","method":"'$METHOD'","params":'"$PARAMS"'}
' \
   -H 'Content-Type: application/json'
```

Note: “Atomic unit” refers to the smallest part of 1 MK implemented according to MKcoin. 1 MK = 1e12 atomic units.

This list has been updated on the merge submission bb30a7236725e456138f055f96a634c75ce2b491 freeze code and updated at block height 1643308.

5.3MKcoin blocks.cpp Code example

```
#include "blocks.h"

#include <unordered_map>

extern const unsigned char checkpoints[];
extern const size_t checkpoints_len;
extern const unsigned char stagenet_blocks[];
extern const size_t stagenet_blocks_len;
extern const unsigned char testnet_blocks[];
extern const size_t testnet_blocks_len;

namespace blocks
{

const std::unordered_map<cryptonote::network_type, const epee::span<const
unsigned char>, std::hash<size_t>> CheckpointsByNetwork = {
{cryptonote::network_type::MAINNET, {checkpoints, checkpoints_len}},
{cryptonote::network_type::STAGENET, {stagenet_blocks, stagenet_blocks_len}},
{cryptonote::network_type::TESTNET, {testnet_blocks, testnet_blocks_len}}
};

const epee::span<const unsigned char>
GetCheckpointsData(cryptonote::network_type network)
{
const auto it = CheckpointsByNetwork.find(network);
if (it != CheckpointsByNetwork.end())
{
return it->second;
}
return nullptr;
}

}
```


Chapter 5 References

[1]http://bitcoin.org.

[2]https://en.bitcoin.it/wiki/Category:Mixing Services.

[3]http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization.

[4]https://bitcointalk.org/index.php?topic=279249.0.

[5]http://msrvideo.vo.msecnd.net/rmcvideos/192058/dl/192058.pdf .

[6]https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki#Specification.

[7]https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#Backwards Compatibility.

[8]https://en.bitcoin.it/wiki/Mining hardware comparison.

[9]https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[10]http://luke.dashjr.org/programs/bitcoin/files/charts/branches.html.

[11]https://bitcointalk.org/index.php?topic=196259.0.

[12]https://en.bitcoin.it/wiki/Contracts.

[13]https://en.bitcoin.it/wiki/Script.

[14]http://litecoin.org.

[15]Mart ´ ın Abadi, Michael Burrows, and Ted Wobber. Moderately hard, memory-bound func- tions. In NDSS, 2003.

[16]Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Ad -hoc-group signatures from hi- jacked keypairs. In in DIMACS Workshop on Theft in E - Commerce, 2005.

[17]Man Ho Au, Sherman S. M. Chow, Willy Susilo, and Patrick P. Tsang. Short linkable ring signatures revisited. In EuroPKI, pages 101 –115, 2006.

[18]Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo -Yin Yang. High-speed high-security signatures. J. Cryptographic Engineering, 2(2):77 – 89,

2012.

[19]David Chaum and Eug`ene van Heyst. Group signatures. In EUROCRYPT, pages 257–265, 1991.

[20]Fabien Coelho. Exponential memory-bound functions for proof of work protocols. IACR Cryptology ePrint Archive, 2005:356, 2005.

[21]Ronald Cramer, Ivan Damg ˚ard, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In CRYPTO, pages 174 –187, 1994.

[22]Cynthia Dwork, Andrew Goldberg, and Moni Naor. On memory-bound functions for fighting spam. In CRYPTO, pages 426–444, 2003.

[23]Eiichiro Fujisaki. Sub-linear size traceable ring signatures without random oracles. In CT- RSA, pages 393–415, 2011.

[24]Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In Public Key Cryptogra- phy, pages 181–200, 2007.

[25]Jezz Garzik. Peer review of "quantitative analysis of the full bitcoin transaction graph". https://gist.github.com/3901921, 2012.

[26]Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). In ACISP, pages 325–335, 2004.

[27]Joseph K. Liu and Duncan S. Wong. Linkable ring signatures: Securit y models and new schemes. In ICCSA (2), pages 614–623, 2005

[28]Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In IEEE Symposium on Security and Privacy, pages 397– 411, 2013.

[29]Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. Structure and anonymity of the bitcoin transaction graph. Future internet, 5(2):237 –250, 2013.

[30]Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In CRYPTO, pages 324–337, 1991.

[31]Marc Santamaria Ortega. The bitcoin transaction graph — anonymity. Master’ s thesis, Universitat Oberta de Catalunya, June 2013.

[32]Colin Percival. Stronger key derivation via sequential memory -hard functions. Presented at BSDCan’ 09, May 2009.

[33]Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. CoRR, abs/1107.4524, 2011.

[34]Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In ASIACRYPT, pages 552–565, 2001.

[35]Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph.

IACR Cryptology ePrint Archive, 2012:584, 2012.

[36]Meni Rosenfeld. Analysis of hashrate-based double-spending. 2012.

[37]Maciej Ulas. Rational points on certain hyperelliptic curves over finite fields. Bulletin of the Polish Academy of Sciences. Mathematics, 55(2):97–104, 2007.

[38]Qianhong Wu, Willy Susilo, Yi Mu, and Fangguo Zhang. Ad hoc group signatures. In IWSEC, pages 120–135, 2006.

Chapter VI Risk Warning

Digital assets are innovative investment products, market price fluctuations will be relatively large, and the management team promises to operate related assets on the principles of openness, transparency and truth. Please rationally judge your investment ability and make investment decisions with caution.