CCE Concrete Coin White paper

Catalog

1. Project background

1.1 Defects of traditional currencies

Milton Friedman, a famous economist, once pointed out that "monetary theory is first and foremost a theory about the demand for money". In monetary theory, there are all kinds of money demand model, but not with money supply model Ms = m. B corresponding money demand model, so use which model can accurately calculate the currency demand, the white box in the money supply and money demand this black box is always not consistent, currency imbalance phenomenon often happens. This is a major flaw in monetary theory.

How to solve the problem? In the context of blockchain technology, many people don’t only see enormous markets but also see the hope in solving the problem of mastering the technology of the circulation and payment industry. Blockchain technology has quickly become the most concerned new technology, owing to its decentralized, trustless, low-cost, natural settlement and other characteristics. The proof-of-concept and application of blockchain technology have begun in almost every industry. A large number of financial institutions and fintech companies have made bold attempts in payment and circulation such as cross-border acquisition, cross-border remittance, foreign exchange settlement and sales. Blockchain technology has the most powerful revolutionary potential in the application prospect of circulation payment.

The traditional circulation payment has some defects which cannot be ignored. The main problems are complicated process, many steps, long transfer time and handling fee. Because of the lack of trust, it is difficult for traditional technologies to solve or break through these problems. Through the blockchain technology, the digital wallet has a wide range of application scenarios, and it has obvious advantages: due to the characteristics of decentralization, once the assets are issued on the blockchain, the subsequent circulation links will no longer rely on the original issuer system, become

open circulation, which will greatly improve the circulation efficiency of digital assets. It almost make up for most of the shortcomings of traditional currencies.

1.2 The blue ocean of mobile payment industry erupted

In the era of Internet financial, mobile payment is a major innovation in the payment industry. As a new and convenient payment tool, mobile payment plays a very important role in the payment industry. Mobile payment not only fills the gap of traditional financial payment service in Internet service, but also becomes an important part of information communication service and financial service system in the era of network economy.

As payments become more immediate, intangible and free, 15 per cent of the industry's global payments revenue -- $280bn -- is likely to be replaced by digital payments growth and non-bank competition, according to a new report from Accenture.

2. Defects of blockchain digital currency

The current cryptocurrency world has its origins in Bitcoin, and every "pure" cryptocurrency has often been associated with a change in one of bitcoin's shortcomings, either through a consensus mechanism, transaction speed, transfer fees, or lack of anonymity. In short, the cryptographic world thrives on bitcoin's quirks.

2.1 Defects of digital currency

1) POW wastes resources

This debate has been going on since the birth of Bitcoin, which now consumes more electricity each year than a small country does. And all the discussion about the waste of resources on Bitcoin comes from the core consensus mechanism of Bitcoin

-- POW (Power of Work), the workload proof mechanism.

Many people have long complained about the waste of electricity, environmental pollution and high mining costs.

2) Bitcoin is not friendly to intelligent contract and DApp development

Bitcoin has brought blockchain, but due to various restrictions of BTC, large-scale development and application of Bitcoin is not practical. Ethereum founder V God had planned to make Ethereum on the bitcoin chain, and the earliest version of Ethereum was a counterparty-like macro coin on the PrimeCoin chain. But some of bitcoin's core developers may have had more concerns at the time, and it didn't go well. When Vgod wanted BTC to be more open and support the development of smart contracts, it was rebuffed by the Bitcoin core.

3) Slow transfer

The block generation speed (block 1 in 10 minutes) and the block size limit (now default to 1MB) together affect the number of transactions a bitcoin network can handle per second. For Bitcoin, slow transaction times and huge transaction fees can be a weakness. With so much bitcoin transaction data flowing through this narrow channel, the current block space limits the amount of transactions the bitcoin network can handle. As a result, transactions are written to the blockchain much more slowly than when users create them. Over time, the processing and squeeze of transactions can leave users waiting hours to be recorded in a block.

4) The wallet takes up up to 280GB of disk space

From the original 2GB to the current 280GB, the number is still increasing rapidly, and the amount of disk space will increase over time.

2.2 Defects of the second-generation digital currency.

The second generation of cryptocurrency is the digital currency represented by Dash. To complete the support of the whole network, the wallet needs to be online and the server usually needs to be rented, so additional costs are left. The instability of the server leads to the frequent offline of the nodes and the loss of block reward, which means that the establishment of the master node is not a one-off, and long-term attention and maintenance are needed.

Nodes require setup process and professional knowledge. The commonly used Linux system forms obstacles for participants without professional knowledge, which is not conducive to development and dispersion.

At present, no team has completed the development of mobile wallet node building function. Participants need to own computers and have certain requirements on configuration. With the rapid development of society, mobile phones are more common tools in our daily life, and the usage of computers has been greatly reduced. This made it impossible for many people to participate because they did not own computers or did not have easy access to computers, which greatly affected the expansion of consensus.

3. CCE digital wallet assets

3.1 The birth of CCE digital Wallet

Cryptocurrency cohesion currency, or CCE. Stock code: CCE, algorithm: XEVAN, Consensus algorithm: PoS, block size: 2 MB, block time: 60 seconds. Total coin supply :20338228.7300123, block reward - 5CCE annual inflation -14%.

CCE, based on the development of blockchain underlying technology, is a digital wallet that utilizes and improves the blockchain technology and belongs to a global

payment tool. But in terms of specific service functions, CCE has more technological advantages than a regular digital wallet can. Such as speed, cross-border payments and trade flows, cross-border transfer assets anonymous, commodity trading between countries, such as art, let you can under the new economic forms, into more offline application scenarios, links to more trade entities, so as to create more new production mode, production relations and the new profit space. CCE adopts PoS working mode, focuses on off-line Staking, and closely combines cashless, card-free transactions and digital assets. Even CCE can pay without network. Every transfer or payment of CCE will automatically start the flow calculation force mining mechanism of the miner. The system will release corresponding points to each wallet according to the contribution value every day and automatically produce them in the wallet in the form of CCE, which is equivalent to digging out a new CCE. So, the CCE wallet is another miner.

CCE USES smart contracts to record the flow and payment process. In CCE, intelligent deposit contract certificate is a common underlying data. CCE aims to help digital currencies by making it easier for global payment institutions for financial transactions to make extensive transactions using collateral assets on customised blockchains.

3.2 The distribution plans of the CCE

For the CCE allocation scheme, according to the core planning, scientific allocation.

10% new function development and expansion, network maintenance.

20% foundation owned, community self-governed, resolution by vote.

10% will be received free of charge through real name, and distributed in the form of candy through multiple apps, media and publicity parties.

20% for publicity, invite awards.

5% is a developer fund, supporting developers who use CCE as their application base.

35% will be given as a reward.

PoS Equity qualification

UTXO share qualification: 600 confirmations (approx. 10 hours)

Qualification after investment: 600 confirmations (about 600 for 10 hours)

Post-investment eligibility: 100 confirmations (approximately 1.66 hours)

Wallet status: Wallete needs to keep Staking online and unlocked.

3.3 Characteristics of CCE issuance mechanism

Global distribution: the larger the volume, the higher the value, the more stable, so that the holders and promoters of the profit is higher, and then promote more efforts to promote, so that holders are willing to invest more, form a virtuous circle!

Decentralisation: CCE is a digital currency that has no central issuer and is obtained by a fixed algorithm.

Fair Benefit: CCE is the first digital currency that truly rewards the value of money back to its creators! Through CCE's innovative issuing algorithm, currency issuing rights are distributed to currency holders and promoters, so as to realize a fair monetary system in which value creators get value.

Withdrawal at any time: there is no closed period, the exchange matchmaking, you can withdraw at any time.

3.4 The circulating value of CCE

CCE has successfully developed a unique side chain technology, which can not only realize real-time exchange of many mainstream digital currencies on the market and trade on major global exchanges, but also connect various mainstream online and offline application scenarios. Any citizen from all over the world can freely hold CCE for convenient payment and circulation. No matter it is real estate sale, tourism consumption, art auction, national bulk goods transaction, anonymous transfer of assets or large consumption places such as global movie and music theaters, everyone can use CCE payment freely. With the decentralized characteristics of blockchain, CCE removes intermediary Banks, breaks down circulation barriers and generates huge profits.

3.5 The technology advantages of CCE wallet

CCE digital wallet has the characteristics of scarcity, anti-inflation, extremely efficient transfer speed, instantaneous transfer after payment, network confirmation, non-forgery, no need for trust middleman, third party can't control transfer transactions, transaction costs are very low, it is an excellent payment tool.

CCE is encrypted and can be stored and transferred on electronic devices. The biggest advantage of this approach is that it is not controlled by a central institution whose value is determined entirely by market demand. CCE records all transactions and USES private key encryption and point-to-point networks to ensure secure decentralized distribution. Each added data block is a "chain", and the record detection of these data is more efficient, safe and convenient.

The biggest difference between CCE and Banks' traditional approach to cross-border payments is that they use more efficient "payment tracks" or "conduits" than Banks do. When a bank remits money abroad, the "intermediary bank" charges a fee, consuming the payer's time and money. CCE avoids the network of intermediary Banks, achieves the transfer of assets through block chain technology, and generates almost no cost in the whole process.

CCE USES digital currency wallet payment technology. The transaction process USES the wallet address, which has nothing to do with personal identity information. Users can have multiple CCE wallet addresses through multiple network devices. In order to prevent others from tracking personal transaction records through the block, CCE will use a public key to encrypt the transaction process. The CCE wallet will eventually integrate Tor(Onion routing) to prevent IP address leakage, use a three-tier encryption algorithm to hide the user's network traffic, and change the source of transactions by jumping between different servers. CCE is completely decentralized, which maximizes the anonymity of the transaction process and protects the privacy of individuals.

4. The features of CCE wallet

4.1 The main node

The cryptographic community is a people-centric community where people come together to perform various functions to ensure that the system works as efficiently as possible. An encryption node is a person on a cryptocurrency network who is responsible for controlling all the state of the network. Each encrypted network has its own set of modes of operation, so in order for the system to work effectively, nodes are set up to ensure that the network members and users maintain the mode of operation agreed upon by decentralized authorization. One of the most common functions of a node is to confirm transactions over an encrypted network by solving

an increasingly complex mathematical algorithm that gives the node the right to create blocks and keep the chain rolling.

A master node is very different from a regular node on a network. The master node is the cryptocurrency full node that holds a full copy of the blockchain event in real time. The master node is also responsible for other things such as ensuring optimal security and privacy for users performing live transactions and participating in more private transactions to set network standards. Participate in decentralized voting system, Masternodes storage all information network fully integrated and 24 * 7 wallet with block chain network. Masternodes also validates or rejects a new block of new transactions added during the build process. By reducing their energy consumption, they could reduce their energy consumption by nearly 1,500 times. Master nodes are not single in an encrypted network, but they can also communicate with nodes like themselves in a decentralized framework. They are often called

MN. It is important to note, however, that although the functions mentioned above represent the functions of the master node, there may be some differences depending on the Settings of each cryptocurrency.

4.2 Features of wallet

Through cold piling technology, CCE enables Staking reward to be offline, which saves server costs and maintenance troubles. Meanwhile, the builder of the main node saves a lot of time to check and maintain, and ensures that the holder can get the reward fairly and will not forget to bring unnecessary losses due to busy work and life.

After three years of research and development, CCE is the world's first perfect solution to the mobile wallet block award function, which can be used by any mobile phone, which is very conducive to global applications and expand consensus.

CCE mobile wallet is the perfect solution to the ever-expanding disk footprint problem, which is only 100KB and will not increase. At present, all coin wallets need to download synchronized block data, and it will take several weeks to install and synchronize BTC wallet. During the synchronization process, it is necessary to keep the computer on and the network open. CCE mobile wallet technology is the first to install and use without synchronous block.

Block chain pay function has long been criticized, from payment to receipt confirmation number can be completed through blocks, it usually need a few small even for a few days time, this speed cannot meet the demand of payment, the payer sent a coin, but cannot provide goods, makes the block chain pay may exist only in theory. CCE mobile wallet takes only one second to receive payment, fully matching the traditional PayPal, Amazon Payments and Dotpay, which makes commodity transactions and even cross-border Payments easier.

CCE mobile wallet has the function of financial management, and Staking rewards are generated in the asset storage process, so that it has the real features of mobile banking with block chain.

CCE autonomous low inflation, the reward model starts with an annualized rate of 14% in the first year and declines by 10% each year. Anyone can become an investment expert and their assets can be easily preserved and appreciated.

CCE mobile wallet is embedded with multi-currency function, which can add any coin. Working on the in-wallet currency exchange function. You actually do the atomic exchange.

CCE computer wallet zero proof feature, completely anonymous payment, which allows no data to track transactions.

CCE provides node building function and attracts technicians to participate in node building, which increases the stability of network maintenance.

5. Planning and construction of CCE wallet

CCE is not only used in a certain field, but also as an ecological digital chain for super industrial applications. Based on wedge side chain technology and open API interface, CCE can provide diversified services for all related products and merchants of circulation payment. In the future, CCE will continue to extend to more ecological fields.

The underlying technology of CCE has three characteristics:

- Protect users from developers

In CCE, developers have no right to interfere with users and can protect users who use the programs they develop.

- Low access barrier

Anyone can access it, without any technology, using computers or mobile phones.

- All data is exposed by default

Associated participants are perfectly capable of hiding their true identities. But by program design, each participant can view all account balances and transactions.

CCE technical team USES the innovative distributed ledger technology to reshape the Internet service model of circulation and payment, create the Internet infrastructure

of circulation and payment in the whole field, and establish the whole ecosystem of CCE+ global circulation payment application.

CCE adopts the CONSENSUS mechanism of PoS to maximize the audience. Its block base network layer is composed of data layer and network layer. The data layer includes the underlying data block and related data encryption and timestamp technologies, while the network layer includes decentralized networking mechanism, data transmission mechanism and data verification mechanism.

5.1 Digital asset storage for CCE

CCE data only allows member nodes in the system to read, write, and send transactions, and records transaction data together, ensuring the security of data on the chain and user privacy.

As a basic component to support distributed business, CCE can better meet the requirements of multi-peer cooperation and orderly development of compliance in distributed business. For example, CCE is more suitable for inter-institutional transactions and settlement, similar to interbank transfers and payments. CCE can be used to create an internal ecosystem to greatly improve efficiency.

CCE has the advantage of high performance, programmable, and privacy protection. It is a completely decentralized blockchain system. CCE reduces the number of nodes, which enables the system to operate with higher efficiency and lower cost. The number of transactions that can be confirmed per unit of time is very considerable, which makes it easier to land in real scenarios. In addition, a very important feature of CCE is node access control and safety standards support, ensuring certification of access, regulatory rules, compliance with regulatory requirements, and improving transaction speed on the basis of trust and safety.

5.2 CCE ‘s technical solutions

CCE technical solution mainly refers to the extension of the underlying platform, in order to facilitate developers to develop products and applications based on CCE technology, or service providers directly provide customers with solutions for specific business scenarios.

Based on the CCE trusted record, the trusted identity of digital certificates, the trusted behavior of digital signatures, and the trusted relationship of intelligent contracts, the CCE technology is used to anchor a multi-dimensional digital network society, and provide all partners in the network ecology with the capabilities of existence proof, integrity proof, identity proof, timestamp proof, data relationship proof, and voucher registration and circulation.

Distributed billing is one of the core features of CCE, and the CCE wallet acts as a billing node. As the value of CCE is embodied, more and more people participate in competitive bookkeeping, and numerous scattered nodes make THE CCE network more secure.

6.The plan and roadmap of CCE

7. Scenario application of CCE

CCE is continuously developing new solutions in the field of circulation and payment. Any holder of the CCE, through the "transfer" or "sweep code payment", in any two CCE mobile money between payment and circulation, according to the current CCE purse value principles of economics, using the chain blocks the underlying technology, combined with six degrees of segmentation theory, social value, multiplication and so on many scientific use, as long as the CCE wallet "balance" circulation can produce "integration", thus value-added compound interest, multiplication, therefore, CCE scenario-based applications is continuously explore,

and go deep into the various fields.

7.1 Settlement and Liquidation

The traditional transaction mode is that both parties keep accounts separately. After the transaction is completed, both parties need to spend a lot of manpower and material resources to check accounts. Because data is opposite party record, authenticity is difficult to guarantee. The data on CCE is distributed, and each node can get all the transaction information. Once changes are found, the whole network can be notified to prevent tampering. More importantly, with the help of the innovative consensus algorithm, the CCE trading process and the clearing process are synchronized in real time, with the transaction being the transfer of value. Meanwhile, the capital clearing is completed, which improves the capital settlement and clearing efficiency and greatly reduces the cost.

7.2 Cross-border Payments

In the field of payment, the application of CCE helps to reduce the cost of reconciliation between financial institutions and the cost of dispute resolution, thus significantly improving the processing speed and efficiency of payment business, which is especially significant in the field of cross-border payment. At present, the intermediate link required for each remittance is not only time consuming, but also requires a large amount of handling fee. Its cost and efficiency become the bottleneck of cross-border remittance. CCE not only bypasses the transit bank and reduces the transit cost, but also improves the convenience of cross-border remittance and the speed of settlement and clearing due to the secure and low-risk features of block chain, which greatly improves the capital utilization rate. The realization of round-the-clock payment, real-time account arrival and cash withdrawal is simple and has no hidden cost, which also helps to reduce the capital risk of cross-border e-commerce enterprises and meet the demand of cross-border

e-commerce enterprises for timeliness and convenience of payment and settlement services.

7.3 Financial Services

CCE in chain based on the financial system, establish the financial services application scenarios, with block chain technology open, do not tamper with the attributes, for decentralized trust mechanism, develop the potential of the financial infrastructure, in order to achieve all kinds of financial assets, such as shares, bonds, bills, warehouse receipt, fund share can be integrated into the chain block books, become a digital assets on the financial system on the chain, and through the CCE in the chain of blocks on the storage, transfer and trading. CCE application scenarios focus on cross-border payment, insurance claims, securities trading, notes and other aspects. Take cross-border payment as an example. Through RTXP protocol and block chain technology, direct interaction can be established between cross-border recipients and payers to simplify the processing process, realize real-time settlement, improve transaction efficiency and reduce business cost.

7.4 Commercial property

CCE USES blockchain technology to record and track land ownership, lease, lien and other information, and to ensure the accuracy and verifability of relevant documents. As a digital currency that can connect global currencies, CCE can realize paperless commercial real estate and real-time transactions. In terms of specific operation, the application of CCE technology in housing property right protection can reduce the time of property right search, realize property right information sharing, avoid fraud in the process of real estate transaction, and improve the operation efficiency of the real estate industry.

7.5 Online Entertainment

CCE is open to all games through the platform API. CCE's fast and convenient payment system and intelligent mechanism of intelligent contract can realize the distribution of the item transaction, which enables CCE online entertainment to have advantages such as encrypted virtual property, decentralized payment and free transaction of items. Independent settlement, independent operation, protection of players, fairness and no change to the original game system, these will become CCE online entertainment from the traditional system unique.

8. Commercial value of CCE

8.1 The market for cross-border payment is sizeable

With the continuous development of economic globalization, trade liberalization and market diversification, countries have become more and more closely connected with each other, economic and trade cooperation has become more and more extensive, and cross-border payments have become more and more frequent. Asia is now the world's largest economy with the greatest growth potential, and its Asia-Pacific region ranked first in the world in 2018 with cross-border payment revenue of us $96.8 billion. Meanwhile, cross-border payment costs remain high, with the average cost for payers reaching 7.68% of the money transferred. With the influx of new players into the cross-border payment market, transactions processed through non-banks have reached 10 per cent of the total size.

8.2 CCE helps traditional circulation and payment

Disadvantages of traditional circulation payment

- Cumbersome process, long settlement cycle: traditional circulation payment is not real-time, the bank end of the day for batch processing of transactions, usually a transaction needs more than 24 hours to complete; Some Banks' cross-border payments seem to be real-time, but in reality, the receiving bank

makes a certain amount of advance payment based on the credit of the remittance bank, and then carries out fund clearing and reconciliation at the end of the day. The business processing speed is slow.

- High fees: The traditional circulation and payment model has a lot of currency fraud, manual reconciliation operation, and reliance on third-party institutions, which leads to high fees. According to McKinsey's "Global Payments 2016" report, the average cost of a cross-border payment through the correspondent bank model is between $25 and $35.

The advantages of applying CCE

- Improved efficiency, lower cost, zero transaction error: after access to CCE, the reliability of data is guaranteed through public and private key technology, and then the purpose of data tamper-proof is achieved through encryption technology and decentralization, ensuring that every transaction is correct. In the traditional circulation payment mode, there are circulation loopholes, payment processing, receiving, financial operation and account checking and other costs. However, the application of CCE can weaken the role of intermediaries in the transaction process, improve capital liquidity and realize real-time confirmation, which can effectively reduce the direct and indirect costs in each link of the transaction.

8.3 CCE and mobile Payment

By eliminating the shackles of the third party and returning data, traffic and value to transaction participants, CCE has overturned the existing offline retail ecosystem through block chain technology and effectively solved various disadvantages of decentralized platforms.

(1) Establish a trusted distributed ledger network

CCE has established a distribution ledger for brick-and-mortar merchants based on blockchain technology, ensured the uniqueness of transactions through a fair and effective consensus mechanism, effectively eliminated problems such as falsification, falsification of data and falsification of orders by centralized platform in order to obtain platform resources, and maintained an ecosystem of fair competition on the whole. Thus, CCE can build true digital trust across the ecosystem.

(2) Fair distribution and circulation of data value

CCE helps merchants and consumers realize the value of their transaction data through tokens and credits. In addition, CCE returns value to its creator by ensuring the true rights of assets, rather than centralizing them through decentralized platform operations. Therefore, data value is disseminated in a more reasonable and equitable way in the physical retail ecosystem.

(3) To realize community consensus mechanism and incentive mechanism

Through the allocation of points to achieve an incentive mechanism, CCE creates a consensus among retailers to share customers and cross-introduce users across fields, and develops corresponding incentive mechanism to cooperate with all parties to contribute to the protection and creation of community consensus, in order to maximize the value cycle of the entire ecosystem.

In addition, CCE brings new opportunities for the application of smart mobile payment in the real economy and reorganizes the physical retail industry. CCE provides merchants with payment functions through intelligent mobile payment via intelligent block chain, creates offline payment portal for CCE, enables consumers to directly use CCE for payment in various payment scenarios in daily life, enables more users to understand, accept and use CCE, and improves the future value and liquidity

of CCE. As smart mobile payment code devices are widely used in physical stores, CCE may provide offline payment gateway. Once adopted on a large scale, it will bring unimaginable huge development space to CCE, including but not limited to the following aspects:

①Set the CCE offline payment standard and become the payment visa of CCE encrypted payment

②Token (CCE) and CCE integral will become the intermediate currency that all other cryptocurrencies can exchange

③Create CCE payment portal.

9. Future development goals and market potential of CCE

Information asymmetry between trading parties in the financial market makes it impossible to establish an effective credit mechanism. There are a large number of centralized credit intermediaries and information intermediaries in the industrial chain, which slows down the system operation efficiency and increases the cost of capital flow. The open, untamable nature of blockchain technology makes it possible to decentralize trust mechanisms and has the potential to transform financial infrastructure, so that its application in the financial sector cannot be underestimated. Payment is the basic link in the financing process. Through the blockchain technology, capital transfer can be realized, especially in the cross-border payment business potential advantage is particularly outstanding, the establishment of direct interaction between cross-border payment and receipt, simplify the processing process, realize real-time settlement, improve transaction efficiency, reduce business costs, thus promoting the development of cross-border payment and other business models. CCE will gradually become the paypal of blockchain.

The potential market

Through the free innovation model and the application of big data, CCE can change the infrastructure of financial market and make capital flow more reasonable. CCE has a large number of data dimensions, such as merchant transaction flow and commodity transaction details, consumers' transaction information, access payment method data, and charging and payment data. Therefore, it lays the foundation for CCE to shift from business focus to data focus in the future. Meanwhile, all information is the basic data of this set of credit data. Great for user and merchant data modeling and portrait work. It takes about 2-3 years from data accumulation to application. With the continuous expansion of the number of users and outlets as well as the continuous increase of data dimensions, a very reliable scoring mechanism will surely be formed for Internet financial companies and other enterprises, which can significantly reduce the application risks of financial products and improve the implementation efficiency of consumers, merchants and financial companies. More importantly, CCE ecology can be provided with its own reliable native scoring system + offline entry, providing irreplaceable on-chain data, consistent with future financial trends. Meanwhile, with the development of CCE chain, market demand will be stimulated to a large extent.

10. CCE R&D team

In May 2017, Brayden Henry, who has rich experience in r&d and management in the field of blockchain technology application, successfully established a world-class blockchain R&D team by introducing global R&D talents and independently developing the most advanced blockchain technology on the basis of drawing up detailed development plans. The team members have experience in the development of Litecoin and international mainstream trading platforms. Brayden Henry led the team to begin core penetration and in-depth research into the ultimate direction of the future digital field. In February 2020, CCE, an innovative

product of The Times, was successfully launched. As the most important link in the blockchain industry chain, CCE application service layer includes various application scenarios and cases of blockchain, including programmable currency, programmable finance and programmable society. The application layer is the underlying technical architecture of CCE application ecology, and the open source programmable application layer provides technical support for the establishment of global blockchain application ecology. CCE is built on the logic of the basic setting based on the future business block chain. Both institutional and individual users can easily build their own intelligent contracts and block chain applications on the CCE.

11.Disclaimer

Participants are required to fully understand CCE, know the overall framework and thinking of the project, and participate rationally before making participation decisions. This white paper is for informational purposes only and does not constitute an opinion on buying or selling CCE. This document does not constitute any investment advice, intention or solicitation. This document does not constitute or be construed as offering any purchase or sale of CCE, nor is it a contract or commitment of any kind. The intended users clearly understand the risks of CCE. Once the investors participate in the investment, they will understand and accept the risks of the project, and they are willing to bear all the consequences. The operations team shall not be liable for any direct or indirect losses resulting from participation in the CCE project.

12. Technical characteristics and correlation

CONCRETE is an open source cryptocurrency focused on fast transactions, with low transaction fees & environmental footprint. CONCRETE is a decentralized sustainable cryptocurrency with near instant full-time private transactions, fair governance and community intelligence.

Name of cryptocurrency: Concrete Coin

Ticker Symbol: CCE

ALGO: XEVAN

Consensus Algorithm: PoS

Block size: 2 MB

Block Time: 60 Seconds

Stake-able: Yes (Earn block reward from coin ownership)

Logo - https://concretecoin.org/downloads/Concrete-wB.png

Total Coin Supply :https://explorer.concretecoin.org/ext/getmoneysupply

Block Reward - 5 CCE Yearly Inflation of -14%

Official website - https://concretecoin.org

Concrete Coin Github address

Concrete coin is an opensource project. The code is available for anyone to contribute and inspect.

Here are the links to Concrete Github

Concrete Coin - https://github.com/CONCRETE-Project/CONCRETE

Concrete Pay - https://github.com/CONCRETE-Project/concretepay

Staking Wallets

Staking can be carried out with the wallets available for Concretecoin. The wallets can be used to monitor and stake by holding some amount of the coins.
The wallet downloads for concrete Apps which include Linux, Windows and Mobile is available from the link https://concretecoin.org/downloads/

API documentation

oncrete API documentation is a technical content deliverable, containing instructions about how to effectively use and integrate with Concrete Coin. It’s a concise reference manual containing all the information required to work with the Concrete Coin, with details about the functions, classes, return types, arguments and more.

Here is the link to access Concrete coin API

https://explorer.concretecoin.org/info

Block-chain browsers

Concrete coin explorer web application allows viewing of addresses, block height, and transactions stored in the blockchain.

The link below are the explorer for Concrete block chain.

https://explorer.concretecoin.org

https://blockbook.concretecoin.org

13. Conclusion

Block chain is pregnant with a huge market space in the direction of cross-border payment/transfer, so CCE is highly valued by investment institutions and capital markets. With the hot trend of block chain technology, CCE is penetrating and promoting in the circulation and payment in the market very quickly. Its circulation scale and velocity are still expanding, and circulation generates value and value increases again, which is the key for CCE to grasp the market. By taking advantage of the non-tampering, transparent, open and node recording features of blockchain technology, CCE continuously improves transaction efficiency and promotes the convenience and security of circulation and payment. CCE has built a large user base through strategic roadshows and expansion.

"Network is an important cornerstone of social development". With the help of value

social networking, media promotion, scene circulation, trading platform and other promotion channels, CCE gradually expands the potential power of network to a more far-reaching capital corner and becomes an application innovator and leader of technology circulation!

Technical appendix

Proof of Stake

CCE use Proof-of-Stake (POS) as part of its mining method, but in particular, the most updated and improved version, PoS 3.0. Proofof-Stake (POS) has proven to be reliable and effective over years of testing and, solving the problems of Bitcoin-derived systems caused by the Proof-of-Work (PoW) protocol. The latest advances in Proof-ofStake are given the new version of PoS 3.0.

The Proof of stake cryptocurrency consensus mechanism explains that for any node to mine or create a block on the network, they must have a certain percentage digital asset.

For the cryptocurrency network to work effectively as a trustless decentralised that it is, then there must be a consensus mechanism that will be in place to guide the operations of every member in the network. On the cryptocurrency network, the personality that ensure that all model of operation are followed to the letter are called nodes. While there are various model of consensus mechanism that can be instilled in the crypto community in this article, we'll be expounding on the Proof Of Stake (POS).

Nodes or miners who are looking to make a fortune on the crypto network must provide services such as confirming transactions in real time that enables the network to work effectively. In the proof of stake mechanism, miners must themselves hold a significant amount of the coin on the network before that are awarded a block. This means that the higher the amount of digital asset a node has, the higher the percentage of possible blocks that can awarded to him. PoS was invented to curb the attack of miners on the crypto network with the belief that if

the nodes have a stake in the network, there's a lower possibility of them attaching the network. It would simply be like stealing from themselves.

A huge amount of energy is needed to mine coin on the crypto network and instead of awarding the block based on the past glory of a miner, POS limits miners to mining only a certain percentage that is in proportion to their ownership stake.

To protect the blockchain network, there are two methods: the first is "Proof-of-Work (POW)" as we talked about previously and the second method is "Proof-of-Stake (POS)". The theory behind PoW is to maintain mathematical competition. The first computer to solve the puzzle confirms the transaction block, wins the currency reward. This is called mining. However, this creates problems of high wasted cost, high energy cost, high fees, slowness (slow transaction processing, slow tx / s) and centralizes the network on some sets of computers belonging to some rich people who could afford all hardware accounts, all because of the very nature of mining.

To compensate for this side created by PoW, we implemented PoS 3.0 in the CCE, which is an improved version of the original PoS and generates competition between coin holders, where, based on network connectivity and random chances, you can confirm a block transaction and receive currency rewards. This is called betting. It requires no specific hardware, except a normal computer with an internet connection, and you will be rewarded in proportion to the coins you have, which makes it fair and decentralized. Currency rewards are determined by annual supply inflation and awarded proportionally to the addresses of that share (equivalent to mining in PoS 3.0).

PoS 3.0 solves Bitcoin's PoW problems, as it is fast and low cost, while remaining decentralized. Below we will see the great security of PoS 3.0 and how it solves related security problems.

Security, coinage and attacks - The whole purpose of competing for coins is to avoid attacks. Confirming transactions is an honor given to a block winner. Although if this system can be used, it will be defective.

In PoS, you first prove that you have access to coins and, from that point on, you

can compete to win blocks at random. The more people competing, the safer the block. The age of the coin is that the longer you hold coins, the more likely you are to win a block. Its original

intention was to encourage inactive coin holders. However, this does not encourage a node to remain connected to the network in practice, as you can expect the reward to increase. In addition, coin holders can disconnect from the network for long periods of time, reconnect and earn enough blocks to risk a 50% attack on the network. Calculating time will affect payments, discouraging connectivity. In addition, the fewer nodes are connected, the easier it will be to obtain most of the blocks that forge consensus. In addition, bets can be calculated in advance to make the attack more effective. Timestamps are used in PoS to get a general idea of the time. Deviation calculations are used to prevent falsifying incorrect time stamps.

In PoW, an increase or decrease in difficulty is made, depending on how quickly a block was produced. However, as a precautionary method to prevent any type of "Timing Attacks", the PoS development system uses centralized checkpoints.

All problems have a solution:

Age of the coin - The age of the coin is calculated by the weight of the unused coins and the time they have been inactive. The calculation is simply "proof of<currency· age· target". The proof hash is the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. The attack to save Coin Age was previously described as unlikely. The reasoning behind this is because it is very difficult to make consecutive double expenses, as Coin-Age would be reset after the first expense. Although this is not entirely clear why an input can be divided into thousands of outputs. This can give the possibility of consecutive double-spending attacks. However, this is still a difficult problem because the attacker would need significant funds to maintain the weight greater than the network. In theory, this makes sense. Although if we look at the number of forks using PoS, we can see that the number of knots is quite low and this gives a much larger weight to a smaller handful of us. A holder of many coins may not want to carry out this attack, as they have the potential to lose the value of their coins if

detected. As rational as this may seem, it is probably a fallacy, because it is still an attack vector 18 and, in fact, very vector. Most importantly, with so many currencies being published daily, keeping as many nodes connected as possible is essential for security.

Pre-computing in Blockchain - Block timestamp is essential for the PoS system. In theory, it is possible to fork a currency by changing the previous timestamps. The stake modifier does not obscure the hash enough to prevent knowledge of future evidence. Therefore, an attacker could try to calculate all the blocks in advance and be more likely to create several consecutive blocks.

PoS 2.0 solution: The bet modifier is changed at each modifier interval to better overshadow the calculations that would be made to identify the time for the next bet proof. The expected blocking time was increased from the original by 60 seconds to match the granularity.

C. Bulk reward - Unfortunately, the bulk reward on most PoS systems is based on the age of the coin. In theory, this is to distribute interest fairly, allowing nodes to receive latent payments due. It is an attempt to maintain a common APR. However, this system does not work because the nodes can remain disconnected and, with many split entries, reconnect to the network and play the reward system. In addition, it offers us no incentive to stay connected. In a decentralized system, the more nodes connected, the better the security, as it transfers the trust of a single entity to the network itself. PoS 3.0 solution: The block reward was made in 20 constant coins per block. This was proportional to the coin supply, maintaining interest at% 1.

Multi-signature and Stake Frio - The final noteworthy addition to the protocol was the implementation of "Multisignature Staking". A disadvantage of many stakeout algorithms is that they only support stakeout with a single key. Since the popularity and use of Bitbay, which uses a two-part guarantee system, also known as "Double Deposit Deposit" and extremely secure double key accounts, it has become important to allow these accounts to participate in protecting the network. Besides dual-key accounts, many other types of entries make use of lock and p2sh times, and these must also be allowed to protect the network. The other problem is that, in a

single key account, a hacker can use keyloggers to obtain your password and compromise your wallet while it is unlocked for stake application.

PoS 3.0 solution: Users could place the block signature key on output "6a", known as the recording address, so they can invest by sending a standard transaction.

This allows any entry to be eligible for submission. The "Cold Stake" technique involves several computers. Basically, when an entry with multiple signatures is eligible for stakeout, the signatures are split between many computers. This makes an account virtually impossible to hack because, even if a single key has been compromised, the other keys are in a completely different location, on the local network or on multiple servers. This technology is also already implemented in the CCE.

What is the difference PoS 3.0 to previous versions?

PoSv3 is really an incremental improvement over PoSv2. In PoSv2, the stake modifier also included the time of the previous block. This was removed to prevent a "short-range" attack, where it was possible to iteratively mine an alternative blockchain, repeating the previous blocking times. PoSv2 used block and transaction times to determine the age of a UTXO; this is not the same as the age of the coin, but the "minimum necessary confirmations" before a UTXO can be used to bet. This has been changed to a much simpler mechanism, where the age of a UTXO is determined by its depth in the blockchain. Therefore, this does not encourage inaccurate timestamps to be used on the blockchain and is also more immune to "timewarp" attacks. PoSv3 also added support for OP_RETURN cointake transactions, which allow a vout to contain the public key to sign the block without requiring a full payment script for pubkey.

- PoS 2.0 solution: Removing the minting from the equation –

"proofhash<coins • target"

-The final noteworthy addition to the protocol was the implementation of the "Multisignature Stak

-We allow users to place the block signature key in output "6a", known as the

recording address so they can bet by sending a standard transaction.

- Massive mining sets and centralizers are not required for PoS; anyone with a computer or cell phone can do it. Therefore, it would be even more decentralized, tending to randomization. Security would benefit and make access and energy efficient easier.

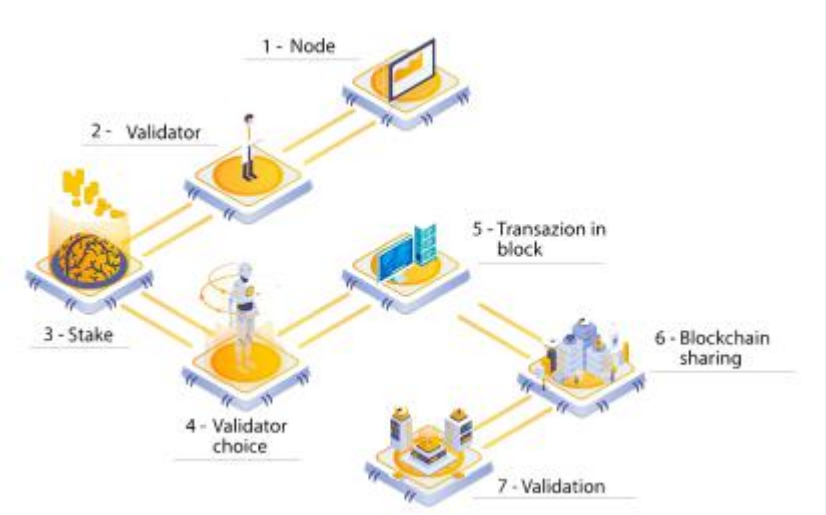
- Big players don't get disproportionately bigger rewards

-More computing power is not useful for creating blocks

-No network member can control the entire blockchain

pseudo-code:

while (blockhash> difficulty) {block.nonce = block.nonce + 1 blockhash = rx16v2 (rx16v2 (block)



This image shows validation process

Eliminating Block Reward based on time was an obvious improvement. Therefore, if the amount of stakeout of nodes falls, the annual interest for active nodes would increase proportionately. For example, if only 1/5 of the network was betting, you can expect up to 5 times the payoff! Unlike many PoS coins that do not have enough knots, this PoS 3.0 feature is a major advantage for small purses. Despite the lack of statistical data on PoS currencies, there are generally less than 20% of participants who bet. In PoS 3.0, the aforementioned increase in incentive will keep the nodes more numerous, more competitive and, therefore, more decentralized. The change in granularity was useful to avoid "stake". Even with all the hashing power of the

Bitcoin network, using PoS 3.0, a practice of attacking the network would be extremely unlikely to the point of being realistically impossible.

PoS 3.0 is one of the most secure and reliable systems ever created and CCE benefits greatly from this new system. Everything is done to guarantee anonymity, keep as many nodes connected as possible, guarantee decentralization and mitigate all attacks. Decentralization was Bitcoin's original core ideology, but unfortunately, Bitcoin's failures prevented it from prevailing eventually. The whole objective of a fair and secure financial system is to put control in the hands of people, so it is for people and for people. Fortunately, PoS 3.0 solved the main problems of Bitcoin's PoW and, at the same time, guarantees its own future by providing an ncentive to stay connected to the network to keep it safe and decentralized

Proof of Work

Consider Bitcoin as an example of a cryptocurrency system secured with a proof of work algorithm. Each block in Bitcoin consists of two parts:

• block header of key parameters, including block creation time, reference to the previous block and the Merkle tree root of the block of transactions

• block list of transactions.

To reference a specific block, its header is hashed twice with the SHA-256 function; the resulting integer value belongs to the interval [0,2 256 − 1]. To account for different possible implementations, use a generic hashing function hash(·) with a variable number of arguments and range [0,M]. For example, arguments of the function can be treated as binary strings and merged together to form a single argument that can be passed to the SHA-256 hashing function.

The block reference is used in the proof of work protocol; in order for a block to be considered valid, its reference must not exceed a certain threshold:

$$\text{hash}(B) \leqslant M/D,$$

where $D \in [1,M]$ is the target difficulty. There is no known way to find B satisfying other than iterating through all possible variables in the block header repeatedly. The higher the value of D, the more iterations are needed to find a valid

block; the expected number of operations is exactly D.

The time period T(r) for a miner with hardware capable of performing r operations per second to find a valid block is distributed exponentially with the rate r/D (see Appendix A):

$$P\{T(r) \leqslant t\} = 1 - \exp(-rt/D).$$

Consider n Bitcoin miners with hash rates r1, r2, …, rn. The period of time to find a block T is equal to the minimum value of random variables T(ri) assuming that the miner publishes a found block and it reaches other miners immediately1 . According to the properties of the exponential distribution, T is also distributed exponentially:

$$P\{T \stackrel{\text{def}}{=} \min(T_1, \ldots, T_n) \leqslant t\} = 1 - \exp\left(-\frac{t}{D}\sum_{i=1}^{n} r_i\right)$$

$$P\{T = T_i\} = \frac{r_i}{\sum_{j=1}^{n} r_j}.$$

;

The last equation shows that the mining is fair: a miner with a share of mining power p has the same probability p to solve a block before other miners. It can be shown that proof of work as used in Bitcoin satisfies Conditions 1–3.

Proof of Stake

In proof of stake algorithms, inequality is modified to depend on the user's ownership of the particular PoS protocol cryptocurrency and not on block properties. Consider a user with address A and

balance bal. A commonly used proof of stake algorithm uses a condition as

$$\text{hash}(\text{hash}(\text{Bprev}),\text{A},\text{t}) \leqslant \text{bal}(\text{A})\text{M}/\text{D},$$

- Bprev denotes the block the user is building on,
- t is the current UTC timestamp.

For various reasons, some cryptocurrencies use modified versions of which we discuss in the corresponding sections.

Unlike , the only variable that the user can change is the timestamp t in the left part of equation. The address balance is locked by the protocol; e.g., the protocol may calculate the balance based on funds that did not move for a day. Alternatively,

a PoS cryptocurrency may use unspent transaction outputs as Bitcoin does; in this case, the balance is naturally locked. A proof of stake protocol puts restrictions on possible values of t. For example, if t must not differ from the UTC time on network nodes by more than an hour, then a user can attempt no more than 7200 values of t. Thus, there are no expensive computations involved in proof of stake.

Together with an address A and a timestamp t satisfying (2), a user must provide a proof of ownership of the address. To achieve this, the user can sign the newly minted block with his signature; in order to produce a valid signature, one must have a private key corresponding to the address A.

The time to find a block for address A is exponentially distributed with rate bal(A)/D (see Appendix A). Consequently, the (2) implementation of proof of stake is fair: the probability to generate a valid block is equal to the ratio of user's balance of funds to the total amount of currency in circulation. The time to find a block for the entire network is distributed exponentially with rate ∑a bal(a)/D.Thus, if the monetary supply of the currency ∑a bal(a) is fixed or grows at a predictable rate, the dfficulty D should be known in advance:

$$D = \frac{1}{T_{ex}} \sum_{a} \mathrm{bal}(a),$$

with Tex denoting the expected time between blocks. In practice, D needs to be adjusted based on recent blocks because not all currency owners participate in block minting.

Sigma Protocol

The Sigma protocol is a mechanism for proving that a statement or occurrence is true. It usually involves two participants; THE PROVER and THE VERIFIER. The prover's aim is to show that the statement or occurrence really is true without showing the verifier the key to understanding the statement or occurrence. The sigma protocol is close to the Zero-knowledge proofs. Although, the sigma protocol can stand alone, it is mostly used as a base for developing the zero knowledge proofs.

Sigma protocol involves a 3-round proof with the following:

1. Message from the prover to the verifier, expressing the fact that he has a truth and that he's willing to have it tested.
2. Challenge from the verifier with a random test to prove that the Prover actually can show the truth.
3. Proof provided by the prover to show that he actually knows and understand the truth without showing the Verifier how he did it.

In the event that the verifier is not satisfied with the fact that the Prover actually knows the truth - maybe the the Verifier thinks the prover just guessed right - then he can put another challenge to the Prover who has to answer by showing the truth and without showing the Verifier how it's done. This process can be carried out again and again with each challenge slimming the chances of the Prover to lie.

The Sigma privacy protocol represents a very important innovation in blockchain privacy, as it combines the high privacy of zero-knowledge proof schemes (ZKP), without many associated disadvantages, bringing great improvements to the CCEChain protocol. It provides an attractive alternative to zkSNARKs, with high anonymity and great performance, but it does so at the cost of reliable configuration, exotic encryption and complicated constructions. Sigma was originally introduced in the blockchain system as the next Zcoin replacement for Zerocoin. Sigma protocol has been introduced in the CCE structure to make significant improvements in relation to Zerocoin in

three areas:

- Reliable configuration removal
- Reduction of the test size from 25 kB to 1.5 kB
- Enhanced security

Sigma is based on the academic article One-Out-Of-Many-Proofs: Or how to

leak a secret and spend a coin (Jens Groth and Markulf Kohlweiss) link: https://eprint.iacr.org/2014/764.pdf , which replaces RSA accumulators using Pedersen commitments and other techniques that cryptographic construction does not require reliable configuration. The only system parameters required in the Sigma configuration are the specifications of the ECC group and the generators in the group. This construction was further optimized in the Short Accountable Ring Signatures document, based on DDH (Jonathan Bootle, Andrew Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth and Christophe Petit) link: https://eprint.iacr.org/2015/643 .pdf that was used to further improve the construction.

Proof and safety sizes

Security through 256-bit ECC curves in Sigma is improved compared to the 2048-bit RSA used in Zerocoin and is estimated to equal the 3072-bit RSA. Our implementation of the CCE also uses the multi algorithms - Pippenger and Straus exponentiation for greater verification efficiency.

Trusted Configuration

Since the beginning of Zcoin, we have always seen the problem of “trusted configuration” as a major drawback. In a trusted configuration, some secret (public) parameters are generated based on a "primary private key". These network parameters are needed to create so-called "zero-knowledge proofs", which is the anonymity technology we use. The “primary private key”, sometimes called toxic waste, needs to be destroyed. If this data is not destroyed, someone with access to that key can generate an infinite amount of anonymous coins. One of the main criticisms of Zerocash and zkSNARKs (which should not be confused with Zerocoin as used in Zcoin), as implemented in Zcash, is its requirement for having a reliable and controversial configuration.

An easy way to view a trusted configuration is to create a box with a lock on it and its corresponding key. Owning the key will allow you to create unlimited treasure from the box and therefore, the key must be destroyed. The trusted

configuration effectively trusts that the key has been destroyed. But how do you know if it's destroyed? Unlike a physical object you can see, destroyed digital objects can always keep a copy or store it somewhere. Therefore, a basically reliable configuration means you need to trust someone or a group of people to destroy the key. If they didn't destroy it or if this ceremony was somehow hidden, someone has that key and can create money out of nothing. Sigma does not require this type of configuration because anyone who wants to help destroy part of the ring can participate.

Zerocoin, implemented by Zcoin, uses a reliable configuration performed by third parties in an academic challenge called RSA Factoring Challenge in 1991, where the incentive to insert a backdoor it is low and there was a considerable reward for breaking it. Although this is a decent implementation and with little chance of being compromised, we believe that the whole purpose of the blockchain is to build systems that do not require trust, and that same principle also applies to our privacy system. The initial launch of Zcoin in 2016 has been delayed, as our founder, Poramin Insom, spent many months trying to remove reliable configurations through the use of RSA UFOs, which proved to be impractical and had to settle for the parameters of the Factoring Challenge of RSA.

Enhanced security

Sigma's safety evidence is fully documented with much simpler construction, making it easier to audit. Sigma removes the reliable configuration and reduces the test sizes from 25 kB to 1.5 kB. The construction of Sigma does not suffer from the same flaw as the Zerocoin Protocol. The Sigma protocol allows users to prove that they have complete privacy in transactions with no reliable configurations through zero-knowledge cryptocurrencies.

Zero-Knowledge Proof (ZKP)

The concept behind the zero-knowledge test is a unique method where a user can prove to another user he knows an absolute value, without transmitting

additional information. Here, the tester can prove that he knows the X value for the verifier without giving him any information other than the fact that he knows the X value. The main essence behind this concept is to prove the possession of knowledge without revealing it. The main challenge here is to show you know a “y” value without saying what “y” is, or any other information.

If a user wants to prove a statement, he must know the secret information. In this way, the verifier could not transmit the information to others without actually knowing the secret information. Thus, the statement must always include that the taster knows the knowledge, but not the information itself. With that, you cannot say the value of "y", but you can say that you know "y". Here, "y" could mean anything.

This is the central strategy of applying the Zero-Knowledge Test. Otherwise, they will not be Zero-Knowledge Proof applications. That is why experts consider the applications of the Zero-Knowledge Test as a special case in which there is no chance to transmit any secret information.

The Zero-Knowledge test must have three different properties to be fully performed. They are:

Completeness - If the statement is really true and both users follow the rules correctly, the verifier will qualify the transaction with no outside help.

Solidity - If the statement is false, the verifier will not allow the transaction to take place in any scenario. (The method is checked to ensure that the probability of falsehood is equal to zero).

Zero Knowledge - The verifier does not store any information.

Exodus

We bring along the entire blockchain system of CCEChain, implementing the Exodus protocol, facilitating the use of smart contracts, personalized currencies/tokens and even decentralized exchange functions. This layer expands the utility and functionality of the CCE blockchain so as not to affect its core functions as a digital currency.

The Exodus protocol is a fork of the Omni protocol (Link: https://www.omnilayer.org/), best known for having Tether built into it. Exodus allows people to build our blockchain protected by an alternative PoW algorithm that, with the next MTP, will be resistant to ASIC.

Briefly, Exodus allows:

- People to create custom tokens on the CCE blockchain

- Blockchain-based crowdfunding

- Distributed exchange for decentralized trading of these tokens CCE has implemented this layer of smart assets in its structure based on the structure implemented by Zcoin.

Dandelion ++

Dandelion ++ is a useful improvement over the original Dandelion protocol. Its integration for the launch of the CCE offers significant improvements in the privacy of the P2P network in the CCE network. Encryption attack vectors continue to evolve, as do solutions for them and Dandelion ++ represents another step forward in protecting user privacy applied to the large CCE system.

The Dandelion ++ protocol is an enhanced version of the Dandelion Protocol (which was originally proposed in 2017), to help improve the privacy of the Bitcoin P2P network. Dandelion ++ addresses concerns with the original protocol and has been implemented by the research team with a positive response from Bitcoin development teams.

Dandelion ++ is a direct network layer solution with anonymity being incorporated into the CCE network, explicitly enhancing the ideals of the original Dandelion proposal and differs from most broadcast communication anonymity protocols in addressing usage objectives and analysis metrics .

To understand how Dandelion ++ works, we must focus on how transactions are transmitted on the CCE network and how the original Dandelion protocol worked. In Bitcoin, when a user transmits a transaction from a node, it is propagated to the nodes connected to that specific node, known as its peers. The

message of the transaction is then propagated in a chain reaction, in which each node spreads the message further to the nodes to which it is connected. This is known as the Bitcoin’s gossip protocol and is how transactions can reach most nodes on the network quickly.

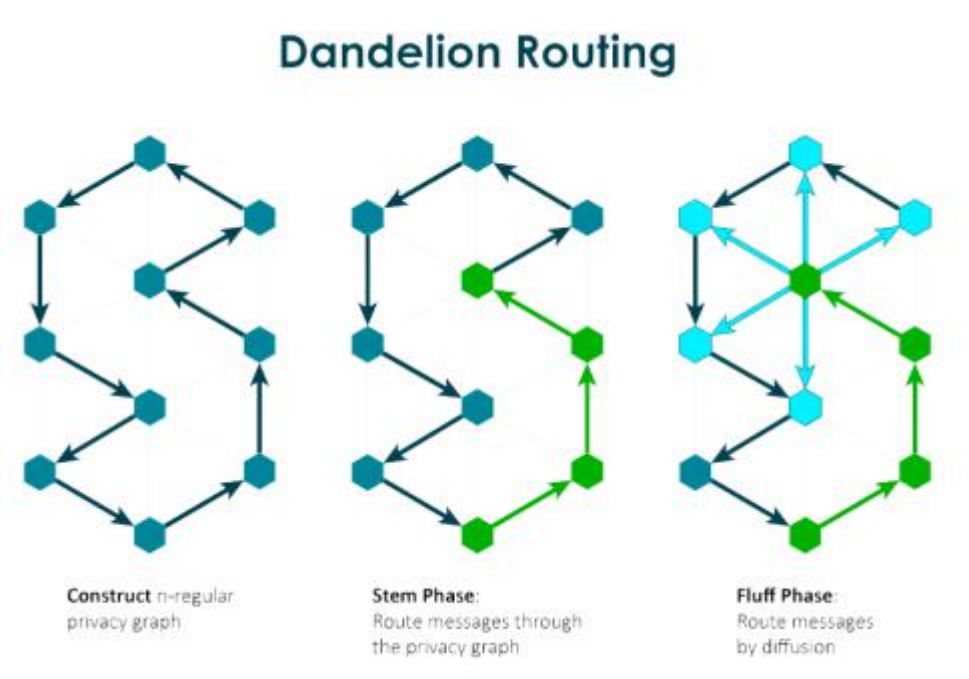
Starting from the Dandelion ++ network, CCE implemented in its network a form of transmission known as diffusion, in which each node spreads transactions with exponential and independent delays to its peers, to mitigate the identification of the IP address of the network users.

Based on normal mapping, the origin of a transaction's sending and its IP address (which is not included in CCE transaction messages) can be mapped by observers if they control enough nodes or use a Supernode connected to many nodes on the network. They can actually map the source address by looking through which nodes the transactions comes from first. The role of Dandelion ++ is, precisely, to make a study of the network and identify it as a Supernode or a major node holder, recorded the traffic relayed from all P2P nodes and observe all patterns of transaction spreads overtime to, occasionally list the source IP address. By linking the IP address to the sender's alias, a third party can disarm users' names and link other transactions, even if a new public key is used for each transaction.

Dandelion was created to mitigate these vulnerabilities, but it had theoretical guarantees that did not apply effectively in practice.

Dandelion's original proposal made three idealized assumptions on this basis:

- All nodes obey the protocol
- Each node generates precisely one transaction
- All Bitcoin nodes run Dandelion—



These assumptions did not work which is why Dandelion ++ tried to resolve them. The initial Dandelion protocol works in 2 phases:

1 - Stem Phase

2 - Fluff Phase

The Stem Phase is the anonymous system where the protocol reduces the possibility of mapping the network back to the IP address of the original node of the transaction message. In the Stem Phase, instead of a node sending a transaction to all connected pairs, it relays the transaction message through the privacy network to a single random pair based on an algorithm. Subsequent to the process, this node transmits the transaction message to another single point in the network, continuing the pattern until eventually (and randomly) a node transmits the message in a typical broadcast format to the rest of the network thus forming a web.

This is where the Fluff Phase begins to interact. After the last random node transmits the message using the network broadcast method, the CCE transaction message is then relayed to most nodes on the network quickly, thus making it much more difficult to trace the original node, as the transaction message it was passed on to many random nodes through a privacy graph before being

propagated to allow the observer to map it to a single node on the network. Instead, an observer could map the propagation transactions back only to the nodes where the message was transferred in the Stem Phase, thus confusing the real identity of the sender of the transaction.

The Dandelion ++ protocol focuses especially on slightly changing the Dandelion implementation options, such as the graph topology and the message forwarding mechanisms within the network. Because of this operation, these small changes in the algorithm exponentially increase the space of the problem state for the analysis of anonymity. Dandelion ++ has increased the information that observers need to track to decode the users' names on the network.

Dandelion ++ differs notably from the original Dandelion in the Stem Phase, where it passes transactions through interlaced paths known as cables before spreading the transaction message to the network. Interlaced paths can be fragmented, but their function when selecting a node to propagate the message is still confined to their local neighborhood. This is an important situation when comparing anonymity solutions at the network level, such as Tor, a routing protocol in which customers need current and global information from the network to determine the paths of transactions.

Dandelion and Dandelion ++ proceed in different cycles. Each node advances when its internal clock in the system reaches a certain limit. For each period, Dandelion ++ works on four main components, with small optimizations:

1 - Anonymity graph:

The anonymity graph uses the random 4-graph system (fig.2) instead of a linear graph system for the anonymity phase, with the choice of nodes whether or not their output neighbors support Dandelion ++ .

2 - Transaction routing (own):

Transaction routing (own) occurs whenever a node generates its own transaction, it forwards the transaction along the same output edge on the regular 4-graph. This differs from one of the problematic assumptions in Dandelion, in which the nodes are assumed only to generate a transaction.

3 - Transaction routing (elay):

Transaction forwarding (elay) is the probability moment in the stem phase when a node receives a stem transaction and retransmits or spreads the transaction over the network. The option to broadcast transactions to the network is pseudo-random. In addition, a node is a diffuser or a relay node for all retransmitted transactions.

4 - Fail-safe mechanism:

The fail-safe mechanism is the place where for each stem phase transaction, each node tracks whether it is seen again as a fluff phase transaction. Otherwise, the node broadcasts the transaction.

With these small adjustments in these stages of the algorithm, they make it more difficult to map IP addresses from the observation of propagation of transaction messages on the CCE network. The Dandelion ++ protocol continues to identify specific attack attempts that can be used against the original Dandelion protocol, including attempted graphics learning attacks, intersection attacks, graphics building attacks and black hole attacks. With each attack vector, they demonstrate how Dandelion ++ mitigates them with theoretical analysis and simulations.

Dandelion ++ does not increase the latency of the CCE network, and its practical feasibility has been demonstrated on the main Bitcoin network. It provides a lightweight and effective CCE network layer anonymity tool to reduce the possibility of mapping attacks to deanonymize users. Despite its advantages, Dandelion ++ does not explicitly protect against opponents at the ISP or AS level, who can use routing attacks to discover a user's primary source on the network.

TOR Integration

TOR (initially The Onion Router) is an open-source software developed several years ago by the United States government, for the military, and later released for use by the population, TOR briefly creates encrypted “tunnels” of traffic overlying the internet, to provide privacy to the user.

The Tor community with the Crypto community, shared the ideal of privacy and decentralization. And in 2017, researchers from the University of Waterloo and the University of Concordia, both from Canada, introduced a system based on blockchain technology using onion routing techniques to facilitate anonymous deliveries.

In a simplified way, the system works as follows:

Within the network, the TOR protocol finds an Entry Node in the network (or Entry Node) which is the initial connection node to the encryption protocol. The Entry Node is the place where CCE transaction data will enter the TOR network securely and anonymously. Between your computer and the Entry Node, a TLS (Transport Layer Security) tunnel is created. This tunnel is highly secure, no one can see what is going through it, all network traffic is encrypted from end to end. Will connect to another node within the network (Secondary Node) where a secure connection is established between two nodes creating a new cryptographic key (Key 2). There can be many Secondary Nodes in the network, the more flexible the network is. This Secondary Node connects to another node (Output Node) that will be where the data will leave the TOR network. The Secondary Node will then generate a new cryptographic key (Key 3) between it and the Outgoing Node, making sure that every transaction between them remains encrypted and secure.

Upon completion of all connections and data transaction between nodes, the Outgoing Node sends a request to its destination address, stating that all data has been individually encrypted by each Node. The server that received the request will know only that the request came from the Outgoing Node, but it will not be possible to track the route of connections and information exchanges traveled between other nodes in the network. Consequently you will not know where the initial transaction was sent from.

The final result obtained within the chain is that each node will know only the request sent through the node before its connection and the Login Node (which is the initial connection node) recognizes only your computer but does not know

the destination of the data. This way, the network encodes its IP addresses between different connections, making tracing or identifying the principle of the transaction invisible.

Comparison Dandelion++ and TOR System

Tor's integration at the network layer level of cryptocurrency systems is extremely challenging. Monero is an excellent example of this, as it took four years to implement his Tor-like I2P Kovri project on his network and it is still a work in progress. Many cryptographic networks do not have the time or technical knowledge to integrate this functionality into their system.

Users who transmit their transactions via Tor, are not viable for ordinary network users like Bitcoin, unaware of the privacy deficiencies of the network or do not have the experience necessary to transmit transactions via Tor properly. in addition, the Tor system can be slow due to limited bandwidth compared to the Dandelion ++ protocol.

In addition, studies have identified concerns about bitcoin spreading animation. It also highlights attacks on us where they reject or blacklisting Tor network connections. This can lead to transaction cancellation and mapping of users' IP addresses making them vulnerable in the network.

Zero-Knowledge –Definition

Definition 1 (Zero Knowledge) Let (P,V) be a interactive proof for L $\in$ NP, with witness relation RL. (P,V) is zero knowledge if for all probabilistic polynomial time machines V $*$ there exists an expected PPT S such that for all nonuniform PPT D there exists a negligible function ε such that $\forall$x $\in$ L,w $\in$ RL(x),z $\in$ {0,1}$*$, D distinguishes the following distributions with probability ε(|x|):

{V iewV $*$[P(x,w) $\Leftrightarrow$ V $*$(x,z)]},{S(x,z)}.

Perfect zero knowledge is exactly the same except that it requires the two distributions to be identical rather than simply indistinguishable.

1. An alternative definition is to replace V IEWV $*$ with OUTPUTV $*$. The two definitions are equivalent, since the

output is included in the view and since V ∗ could simply output its view.

Definition 2 (Zero Knowledge) Let (P,V) be a interactive proof for L ∈ NP, with witness relation RL. (P,V) is zero knowledge if there exists an expected PPT S such that for all probabilistic polynomial time machines V ∗ and for all nonuniform PPT D there exists a negligible function ε such that ∀x ∈ L,w ∈ RL(x),z ∈ {0,1}∗,r ∈ {0,1}∗, D distinguishes the following distributions with probability ε(|x|):

{V iewV ∗[P(x,w) ⇔ V ∗(x,z)],r},{S Vr∗(x,z) (x,z),r}.

Definition 3 (Commitment Scheme) Com is a commitment scheme if Com is polynomial time and there exists a polynomial `

such that the following two properties hold:

Hiding: For every nonuniform PPT D there exists a negligible function ε such that for all n ∈ N, v0,v1 ∈ {0,1} n , D distinguishes the following distributions with probability at most ε(n):

{r ← {0,1} `(n) : Com(v0,r)},{r ← {0,1} `(n) : Comm(v1,r)}.

Binding: For all v0,v1 ∈ {0,1} n , r0,r1 ∈ {0,1} `(n) , if v0 6= v1 then Com(v0,r0) 6= Com(v1,r1).

Commitment schemes can be constructed from OWPs (or OWFs):

Lemma 4 If one-way permutation exist, then there exist (perfectly binding) commitment schemes.

Proof. We begin by constructing a single-bit commitment scheme. Let f be the assumed one-way permutation, and let h be a hard-core predicate for f. We define a commitment scheme by:

Com(b;r) = (f(r),h(r) ⊕ b).

Zero-Knowledge –Proof

Proposition 1 If (P,V) is a ZK protocol, then (P,V) is witness indistinguishable.

Proof. By definition of ZK, there exists a simulator S, such that:

{P(x,w1) ↔ V ∗(x,z)} ≈ {S(x,z)} ≈ {P(x,w2) ↔ V ∗(x,z)}

By the hybrid lemma, {P(x,w1) ↔ V ∗(x,z)} ≈ {P(x,w2) ↔ V ∗(x,z)}. So (P,V) is witness indistinguishable.

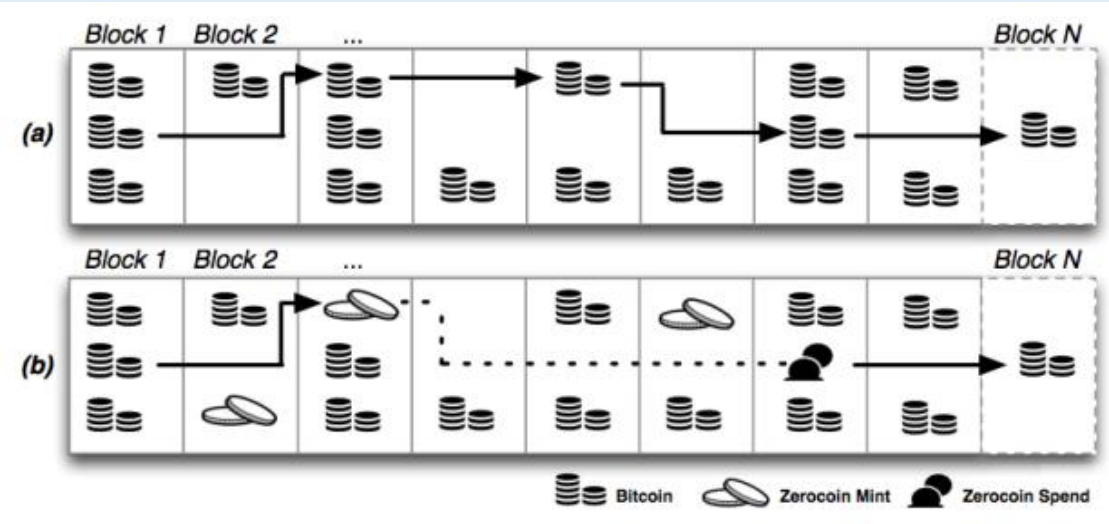
Finally, here is the theorem that says why Witness Indistinguishability is nice to work with.

Theorem 6 If (P,V) is WI, then (P n ,V n) is WI. In other words, WI protocols can be repeated polynomially many times in parallel and still be WI.

Proof. We want to show that {P n(x,w1) ↔ V ∗n(x,z)} ≈ {P n(x,w2) ↔ V ∗n(x,z)}. To do this, define the following hybrids: Let Hi denote the view where the prover uses w1 for the first i executions of the protocol, and w2 for the rest. Then it is clear that our problem is exactly showing that H0 ≈ Hn. If they were distinguishable, then by the hybrid lemma, some Hi 6≈ Hi+1. However, I claim that this is not possible by efficient operations. Because the prover is efficient, we can efficiently simulate the entire protocol where the prover uses w1 and output the view. We can do this i times. Likewise, we can efficiently simulate the entire protocol where the prover uses w2 and output the view. We can do this n − i − 1 times. So concatenation by views of a WI protocol for a fixed witness is an efficient operation. Now observe that Hi is exactly {P(x,w1) ↔ V ∗(x,z)} with i copies of the view of {P(x,w1) ↔ V ∗(x,z)} pre-concatenated, and n − i − 1 copies of the view of {P(x,w2) ↔ V ∗(x,z)} concatenated. Next, observe that Hi+1 is exactly {P(x,w2) ↔ V ∗(x,z)} with i copies of the view of {P(x,w1) ↔ V ∗(x,z)} preconcatenated, and n − i − 1 copies of the view of {P(x,w2) ↔ V ∗(x,z)} concatenated. So because (P,V) is a WI protocol, {P(x,w1) ↔ V ∗(x,z)} ≈ P(x,w2) ↔ V ∗(x,z)}, and by efficient operations, Hi ≈ Hi+1. So we cannot have any Hi 6≈ Hi+1, so we have H0 ≈ Hn, and (P n ,V n) is also a WI protocol.

How ZeroCoin Work

Zerocoin allows direct anonymous payments between parties. Zerocoin transactions exist alongside the (non-anonymous) Bitcoin currency. Each user can convert (non-anonymous) bitcoins into (anonymous) coins, which we call zerocoins. Users can then send zerocoins to other users, and split or merge zerocoins they own in any way that



preserves the total value. Users can also convert zerocoins back into bitcoins, though in principle this is not necessary: all transactions can be made in terms of zerocoins.

What makes Zerocoin and the new Zerocash protocol different from previous approaches:

Zerocoin and the Zerocash protocol operates in the Bitcoin network and is implemented as a series of extensions to the existing Bitcoin protocol. This approach means that Zerocoin can be deployed without relying on a central coin issuer or bank (as used in previous e-cash schemes). Moreover, since no single trusted party operates the Zerocoin system, attacks on Zerocoin must take on a substantial fraction of the Bitcoin network.

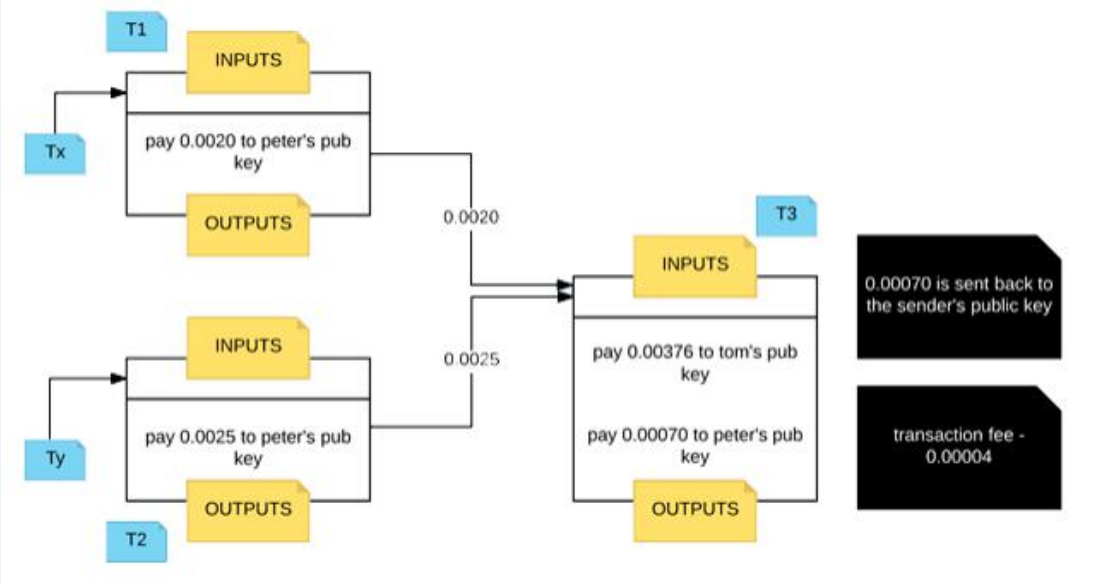
The Zerocash protocol uses provably secure cryptographic techniques to ensure that Bitcoins cannot be traced. These techniques allow users to conduct transactions on the Bitcoin network while receiving strong mathematical guarantees that the transactions cannot be traced. These guarantees remain in place even if a portion of the Bitcoin network is compromised by an attacker.

Other anonymous cash systems rely on distributing the work of anonymizing users amongst a set of parties. This approach works well if all parties are fully available but can be subject to “denial of service” attacks where a small number of nodes are taken offline. Because Zerocoin is built on top of Bitcoin, it is widely distributed among all the Bitcoin peers, ensuring that the system can remain available even when many nodes are compromised.

notation	example	meaning
monospace	Encrypt, challenge	algorithm/procedure/oracle names
$\leftarrow$	$y \leftarrow f(x)$	assignment
$\rightarrow$	$f : X \rightarrow Y$	function definition
$\twoheadleftarrow$	$b \twoheadleftarrow \{0,1\}$	uniform random sampling
$\twoheadrightarrow$	$\mathsf{Encrypt} : PK \times M \twoheadrightarrow C$	randomised algorithm
$\perp$		a special symbol denoting "failure"
$\uplus$	$M \uplus \{\perp\}$	disjoint union (coproduct)
$\mathbb{N}$		natural numbers, including 0
$[\,]$		empty list
$::$	$L \leftarrow L :: l$	append to list

Bitcoin Transaction- technical explanation

The following images show Bitcoin transaction:



How does a bitcoin transaction work?

So if I'm Bob and I want to pay Alice, those inputs are my proof that I have been given a certain amount of money (although this might just be a portion of my total balance), and the outputs will correspond to Alice's account.

Main

hash: The hash over this entire transaction. Bitcoin generally uses hash values both a pointer and a means to check the integrity of a piece of data.

ver: The version number that should be used to verify this block. The latest version was introduced in a soft fork that became active in December 2015.

vin_sz: The number of inputs to this transaction. Similarly, vout_sz counts the number of outputs.

lock_time: Describes the earliest time at which a block can be added to the blockchain. It is either the block height or a unix timestamp.

Input

previous output hash: This is a hash pointer to a previously unspent transaction output (UTXO). Essentially, this is money that belongs to you that you are about to spend in this transaction.

n: An CCE into the list of outputs of the previous transaction. This is the actual output that you are spending.

scriptSig: This is a spending script that proves that the creator of this transaction has permission to spend the money

Output

value: The amount of Satoshi being spent (1 BTC = 100,000,000 Satoshi).

scriptPubKey: The second of two scripts provided in a bitcoin transaction, which points to a recipient's hashed public key.

Transaction verification

The function bitcoin node is the verify that incoming transactions are correct (data hasn't been tampered with, money isn't being created, only intended recipients spend UTXOs, etc).

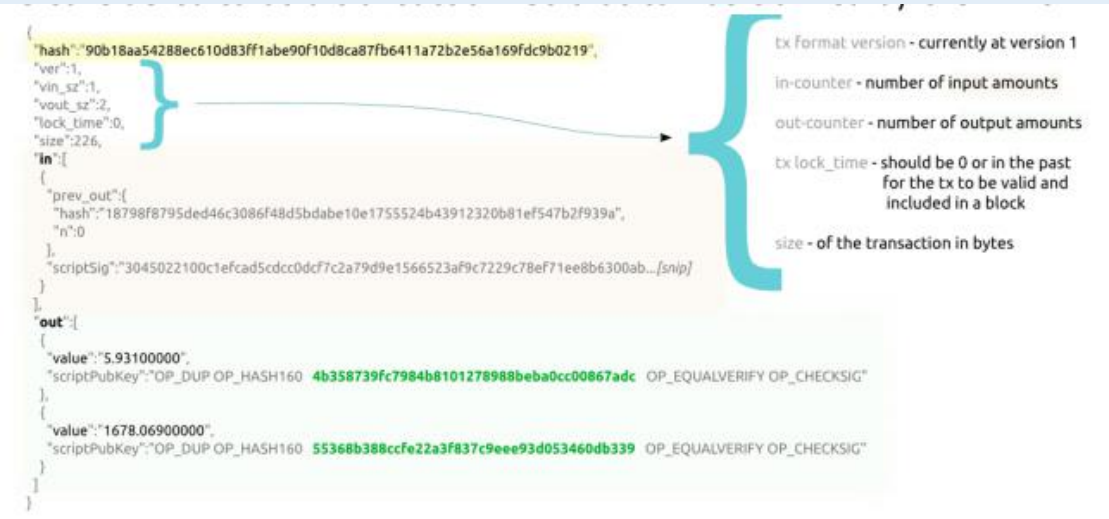
All outputs claimed by inputs of this transaction are in the UTXO pool. Unspent outputs can only ever be claimed once.

The signatures on each input are valid. More precisely, we're saying that the combined scripts return true after executing them one after the other. More on this in the last section.

No UTXO is spent more than once by this transaction. Notice how this is different than the first item.

All of the transaction's output values are non-negative.

The sum of this transaction's input values is greater than the sum of its output values. Note that if the numbers are different, the difference is considered to be a transaction fee that can be claimed by the miner.



In the example, you can find a transaction ID highlighted in yellow. Meta-data along, with a description, is on the right. Inputs and outputs are highlighted in pink and green

Bitcoin Transaction- simple explanation

To understand how a bitcoin transaction works, it is important to understand what bitcoin itself is. Bitcoin ordinarily is an intangible digital asset that was created to carry out the functions of fiat currencies and more. For example, the 'exchange of value' function of fiat. Also, bitcoin is not a single unit coin but more like a file (which represents money) that is moved when a payment or receipt transaction is initiated.

There are three major components of every bitcoin transaction and that includes: The Input, The Output and the registered amount.

The Input

The input transaction represents the address or source of the bitcoin. Such that for every collection of bitcoin unit that is transferred from one source to another, an address of where it originated from is stated. This ensures that every single movement of the littlest amount of bitcoin all goes into a proper immutable record including where they came from.

The Output

The output transaction is simply the other end of the input transaction. The output represents and codifies all necessary information about the receiver of the bitcoin. To receive any amount of bitcoin, you'll have to generate a receiving or output address from your end and send that address to the person who is going to initiate the sending or input transaction. The sender then copies your unique receiving address and initiates that the bitcoin be sent to that address. The output address is more like your bank account number for receiving funds. It is important to note that a single tweak in an output address makes it totally unrecognized in the bitcoin network.

The Amount

For every transaction of bitcoin made, there is a deliberate effort made to enter how many unit of bitcoin is sent or received. It is possible to receive a tiny fraction of bitcoin in a transaction while it is also possible to send huge numbers of bitcoin in a transaction. The system is built in such a way that the bitcoin can be broken down beyond the unit of one (1) meaning that you can send 0.5 bitcoin or even 0.005 bitcoin.

Bitcoin Transaction

When you send bitcoin to someone, your address is saved on the bitcoin network relating to that amount of bitcoin you sent. So also, when you receive bitcoin from another party, your address is stored on an inaccessible record. The record of transactions to and fro enables every unit of the bitcoin in circulation to be accounted for. In fact, it means that if transactions are to be traced, we can do a genealogy research of who made the very first bitcoin transaction and to whom it was sent.

HOW AND WHY BITCOIN ADDRESSES ARE CHANGED AFTER EVERY TRANSACTION.

The bitcoin network is a system and so is the entire unit of bitcoin in the network. The way the system was built makes us know that all units bitcoin available on the network is like a loaf of bread. When you share out of this loaf, you give it an entirely different identity when it reaches its destination. More importantly, a new address is generated to incorporate the bitcoin unit you sent and the units the receiver has in

his wallet before yours joined. These are two loafs, from the same origin coming together, again. And they take another identity and become a whole.

Just like when you send $5000 dollars to someone who has $2000 IN their bank account before. When the transaction is completed, the beneficiary will have a while $7000 IN their account even though there is a record of how the $7000 came to being.

Also, after every transaction from the sender, the remaining bitcoin balance he has generates a new address. To ensure this, when sending a bitcoin unit, a sender is made to send the whole unit of bitcoin he has and then the bitcoin network then spilt it within the sender and the receiver. For instance, if I have 1 bitcoin and I want to send 0.5 of my bitcoin to someone, once I initiate a 0.5 transaction, my entire one bitcoin is lifted and divided into two and one part is sent to the other back to the senders wallet.