!
Whitepaper V.0.8.5

Hcash

The New Standard of Value

Table of content

I. Executive Summary

Hcash is the cryptocurrency of a distributed ledger which links block-based and blockless blockchain systems

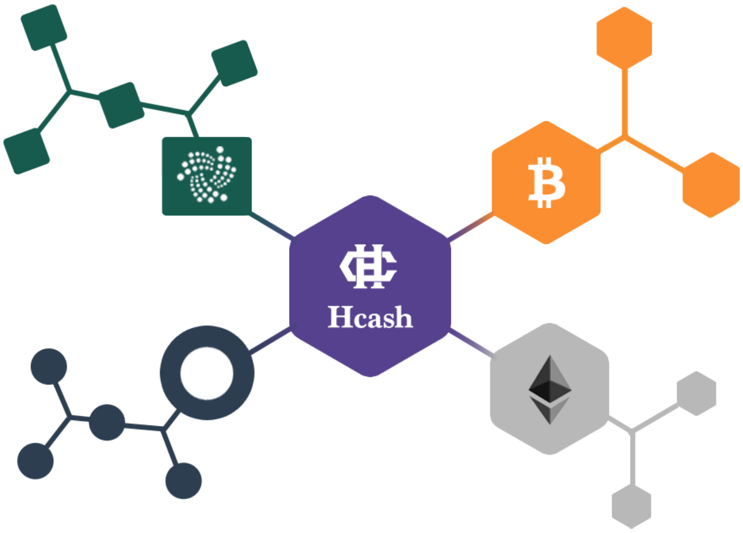
The UTXO-based blockchain system (e.g. Bitcoin [1]) and account-based blockchain system (e.g. Ethereum [2]) has opened the door of a brand-new world for us. Although the impressive success of Bitcoin and Ethereum has certainly proven the value of blockchain technology and its massive potential in the future, we also see some inherent problems in blockchain technology along the way. Since 2015, there has been quite a few highly-promising distributed ledger systems that are not block-based gradually coming into our view, such as DAG (Directed Acyclic Graph) [3]. With no doubt, a decentralized digital world is dawning, and Bitcoin or Ethereum has the potential to become the base currency in block-based distributed ledger. IOTA [4] or Byteball [5], on the other hand, may fulfil a similar role in a system based on DAG technology. Nevertheless, despite of the ability to be traded unrestrictedly on some centralized exchange platforms, these tokens, due to the fundamental differences in the underlying systems, can only circulate within their own blockchains, and would not be able to move freely from blockchain-based to blockless system or vice versa.

Our intention is to create a new decentralized and distributed ledger system that will bridge the gap between blockchain-based or blockless systems, thereby allowing value and information to be circulated freely between different blockchains. In addition, just as Bitcoin serves as the tools of exchange for goods or services in blockchain-based system, we also need a type of asset in the newly invented system that can reflect the value of goods or services objectively. As to the new store of value, we call it “HyperCash” (hereinafter referred to as “Hcash”)

II. Introduction

In our vision, Hcash will create a new platform that can be connected to different blockchains (such as Bitcoin blockchain and Ethereum blockchain), thereby allowing value and information to circulate freely among systems, and redefining the value of blockchain.

Below is a schematic diagram of the Hcash platform.



A. Hive: Composed of Blockchain and DAG systems

Hcash platform is designed to be the sidechain for both blockchain-based and blockless systems, so it can achieve free flow of value and information between the two. Here, Hcash is the medium for cross-platform value exchange, while the platform itself is carrier for cross-platform information interflow.

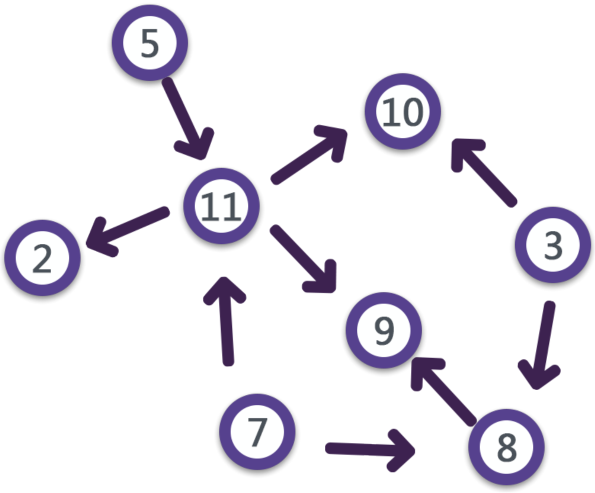
Based on these design features, Hcash has taken into account the reading of information from blockchain-based (including UTXO and Account Based) and DAG based distributed ledger at the initial stage of system design.

Address system

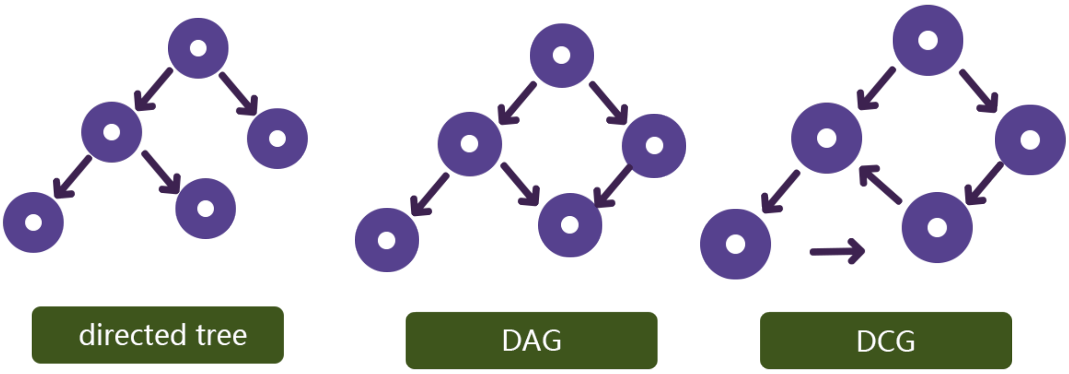
In order to implement another important feature that will be discussed later, Hcash is designed purposely to have both public and private addresses to be compatible with Zcash (t-addr and z-addr) and Byteball address systems (whiteball and blackball). Therefore, in the near future, it is expected that people can directly send and receive ZEC (or similar) or GBYTE (or similar) from blockchain to DAG system and vice versa in the Hcash platform. Meanwhile, it would also be possible to achieve fully-encrypted communication based on Zero Knowledge Proof technology between Hcash nodes and clients, as well as a range of other exciting new features.

About Directed Acyclic Graph

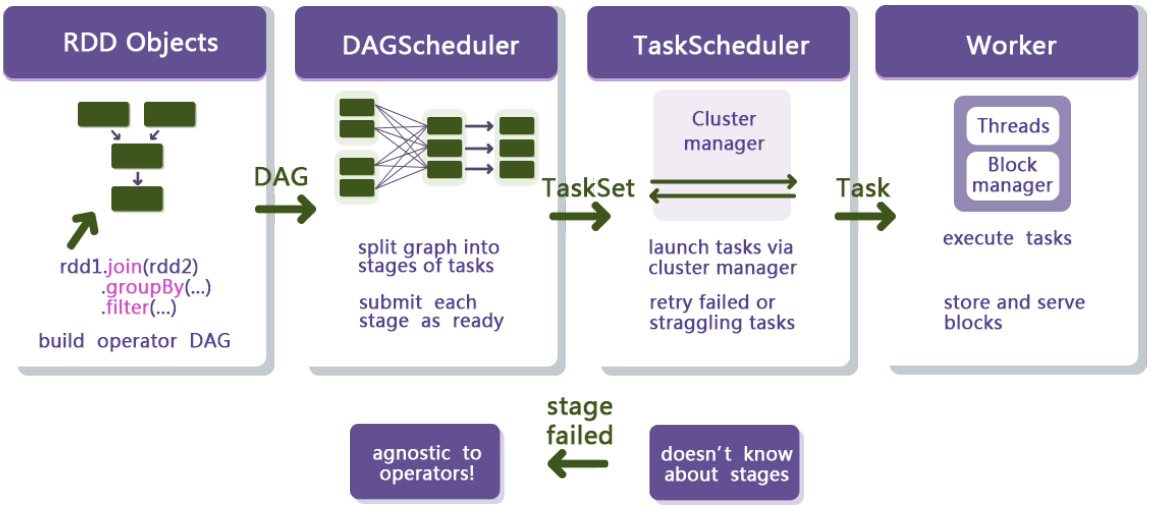
Directed acyclic graph (DAG) is a finite directed graph with no directed cycles. That is, it consists of finitely many vertices and edges, with each edge directed from one vertex to another, such that there is no way to start at any vertex *v* and follow a consistently-directed sequence of edges that eventually loops back to *v* again. Since the path from a starting vertex to an ending vertex in a directed graph might not form a cycle, a DAG is not necessarily a tree, but any directed tree is a DAG



Compared to directed tree, DAG is a special but more general directed graph. Below is a simple illustration of directed tree, DAG and directed graph. In the Big Data industry, DAG is usually used for Big Data framework, such as the execution engine of Hadoop, Storm and Spark.

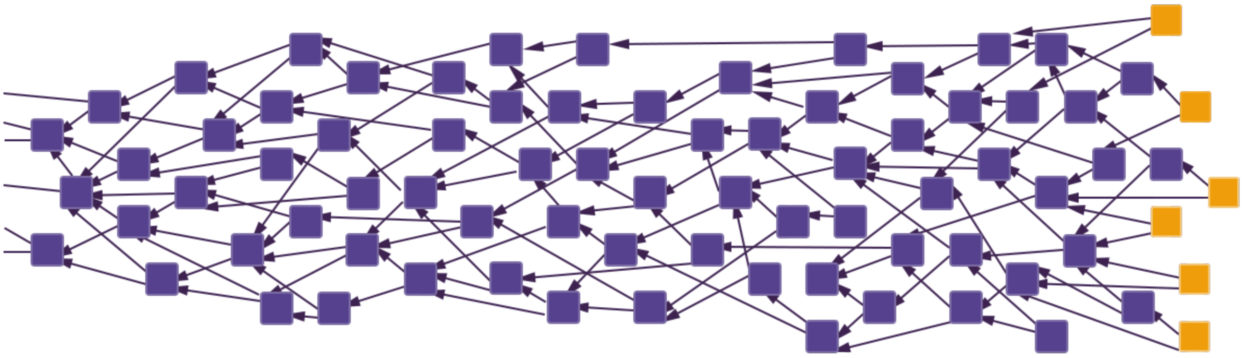


The following graph shows the operating architecture of Spark:

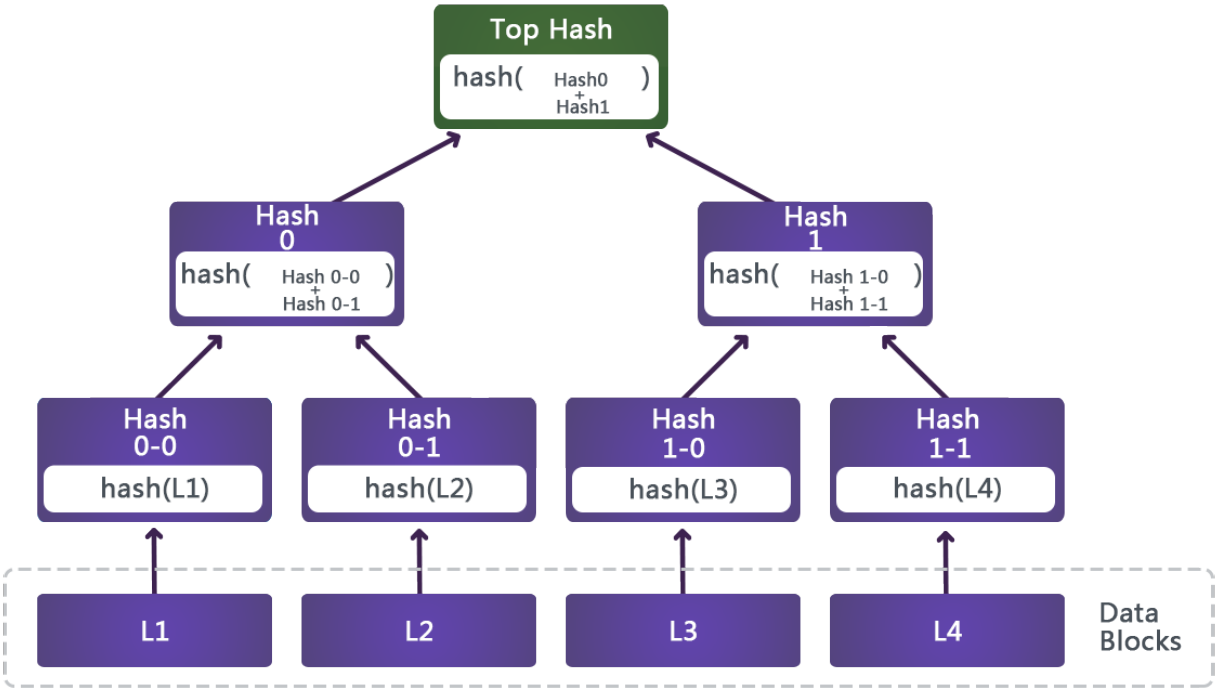


There is a dependent relationship between each RDD object, which forms a DAG. The DAG scheduler will split the graph into multiple "Stages". The rules for partition are simple: scanning through from back to front, whenever the DAG scheduler encounters a narrow dependence, it will be added into current Stage, whereas a wide dependence needs to be shuffled. After completing the division of stages, DAG scheduler will generate a Taskst based on each stage and submit the TaskSet to TaskScheduler. The TaskScheduler is responsible for the scheduling of specific task and execution of tasks on worker nodes.

Recently, with the development of blockchain technology, there are some emerging blockchain systems that used DAG in the underlying data structure, such as IOTA [4]. IOTA's core data structure, called 'Tangle', is a DAG that designed to resolve existing issues in the "Internet of Things" (IoT) industry, such as massive data storage and distributed computing, as well as providing a good solution for the micropayment in the IOT industry.



Traditional blockchains (such as Bitcoin and Ethereum) are using the binary tree data structure such as the Merkle tree:



Hcash attempts to establish a channel between the systems that are based on two completely different data structures, so that it can be compatible with current mainstream blockchain technical standards in the bottom level while allowing new blockchain technologies to be able to communicate with current blockchain systems. Although the challenge is undoubtedly great, Hcash's technology development team consists of renowned cryptographers from world's famous academic institution as well experts from blockchain, Big Data and Cloud Computing industry. Therefore, we are confident that with the support from all these experts, the team will overcome the obstacles and meet the original design goals of the system.

B. Hybrid: PoW + PoS

Achieving consensus across digital currency communities has always been a difficult problem to solve. As we all know, the struggle to upgrade Bitcoin via protocols has been affecting the development of the community over the past two to three years, while the over-centralized governance system adopted by Zcash or similar has certainly deterred active participation across the community. Currently, none of the decision-making process used in this crypto-economics can preserve the system's ability to adapt in the face of technical challenges and accommodate the ideological differences among community stakeholders without compromising the integrity of blockchain's decentralized value proposition

By learning from predecessors and incorporating partially the philosophy of Decred and Dash, Hcash, for the first time, introduces the concept of Instant-Open-Governance, which allows all coin holders to participate in major decisions in the community through PoS mining mechanism, including protocol updates and upgrades. Most importantly, the mechanism adopted by Hcash is more advanced than the traditional voting method in the sense that it provides smoother execution. Once the vote is passed, all decisions will be recorded in the blockchain and enforced, thus avoiding the problem of consensus among miners, mining pools, exchanges and wallet service providers. The introduction of PoW mechanism is to prevent pre-ICO investors from occupying an excessively large portion of rewards in a PoS distribution mechanism. Also, PoW is the security mechanism that has been proved to be the most effective way to protect blockchain-based system. Although it will inevitably consume a large amount of energy, we believe the tradeoff is still worthy in consideration of the security benefits it brings to system. Moreover, it is possible to combine PoW with PoS mining process to enhance the overall security of the system.

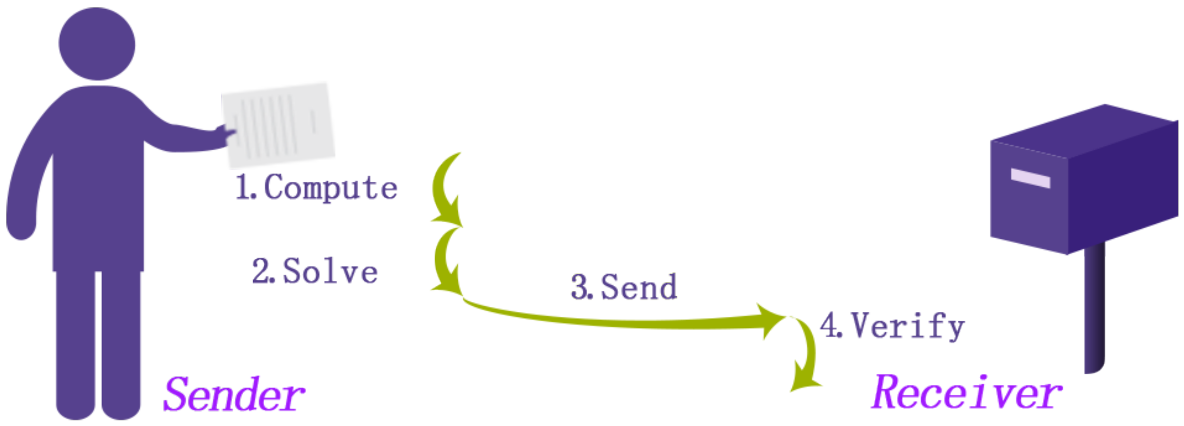
At first, the mining process would begin in a traditional PoW manner where miners would compete to solve a cryptographic problem. According to this implementation, the blocks being mined do not contain any transactions (they are more like templates instead), so the new blocks that are added to the blockchain will only include a header and the winning miner's reward address. At this moment, the system will switch to PoS. Based on the information contained in this header, a set of random validators is selected to sign the new block. Here, the chance of a validator to be selected would depend on the number of coins he or she holds. The more coins a validator has, the higher the probability of him/her being selected. Once these selected validators have completed the signature of the block, the template will become a complete block. If some of the validators are not available for signing the block, they will be selected to sign the next block and a new set of validators will be selected until the current block gets the correct number of signatures. The transaction fee will be distributed among the miner and the validators who participated in the signature of the block.

For PoW [6], a qualified block can be expressed as:

$$f(nonce) < target$$

Where “nonce” is a random element, “target” is a quantification of qualified block, and the “Target” of each accounting node is consistent. In addition, the successful operation of PoW also requires the following two principles:

1. Best chain principle: the longest chain is considered as the correct chain.



2. Incentive principle: rewards will be awarded to those who have found qualified blocks.

Principle 1 is a mandatory rule that must be followed by everyone. The common goal is to find a consistent ledger, and the longest chain represents the greatest workload. If there is no such consensus, everyone will only construct their own chain and no agreement can be reached.

Principle 2 is the workload incentive. Due to the cost of accounting, the only way to encourage people to participate in the network is to provide rewards to them according to the workload.

In this way, participation in the accounting and recording of transaction for the blockchain becomes an investment behavior, and the cost, benefits, and risks involved in the process will naturally form a game under the constraint of principle 1, which drive all the nodes to construct blocks according to the principles faithfully and finally reach a Nash equilibrium.

For PoS [7], a qualified block can be expressed as:

$$f(timestamp) < target * balance$$

The above PoS scheme is currently used by nxt [8] [9] and Blackcoin [10]. The simple version of PoS mechanism can easily lead to centralization of wealth (as the wealthiest participants have the greatest impact and highest chance of being selected as validators), which can pose serious threat to the integrity and security of the whole system. Therefore, we must add another variable into the formula to prevent the problems of centralization and security arising from only considering stake (balance). Compared to PoW, the search space on the left side of the formula is changed from “Nonce” to “Timestamp”. As the range of “Nonce” is infinite, but the range of “Timestamp” is extremely limited, the block time of a qualified block must be within the specified range of the previous block’s block time - blocks that do not meet this criterion will not be accepted by other nodes.

The target value on the right side of the formula introduces a product factor, balance. Therefore, the larger the balance is, the larger the target value is (Target * Balance), and the easier a block is to be found. Because the range of “Timestamp” is limited, the success rate of casting a block through PoS is mainly related to Balance (Stake). Hcash's PoS mechanism will draw on existing PoS mechanism to improve the efficiency of PoS under the premise of ensuring the security of the system, and focus on improving the security of the digital currency when the PoS mechanism is used.

C. Hierarchy: DAO Governance

The Decentralized Autonomous Organization (DAO) is an unexpected, yet ideal product of the cryptography technological revolution. The root of the Decentralized Autonomous Corporation (DAC) can be traced back to the decentralized organization described by Ori Brafman in "Starfish and Spider" (2007) [11], and "peer production" described by Yochai Benkler in “Web Fortune” (2006) [12]. However, these two concepts are later linked together by cryptocurrency-related technology, and gradually entered into cryptocurrency lexicon. In October 2013, Dan Larimer first put forward the idea of Decentralized Autonomous Corporation (DAC), where he considered Bitcoin as a DAC also.

About DAC

In order to provide a clear definition of DAC, we have summarized the seven features that are necessary to a DAC:

- Openness: The design of DAC system is made with a priority for transparency. The principle of openness and transparency is the cornerstone of the entire DAC system. An organization that operates behind closed doors cannot be considered as a DAC. Nowadays, the spirit of open source software has become a typical example of openness.

- Decentralization: No centralized individuals or organizations can control the entire DAC. This feature determines self-similarity. The decentralized characteristic of the system ensures the vitality of the DAC system and protects people from corruption and abuse of authority,

- Autonomy: Everyone can participate in the DAC system. All participants are either subsidiary or sub-unit of DAC system, which will promote the development of DAC from their own point of view. The spontaneous behavior of the participants guarantees the operation of the DAC.

- Value: A DAC system must have use value and can be put into practical application. For example, several features of the bitcoin system, such as international payment network, anonymous transaction, tax avoidance and value storage, have determined the profitability of the Bitcoin DAC system and contributed to improve the value and utility of the coin for coin-holders.

- Profitability: DAC participants will receive rewards for contribution to DAC system development, and the profitability is determined by the value of the DAC itself.

- Self-similarity: Even there are only a few DAC nodes exist, the DAC system can still function and develop normally. The destruction of some unit nodes will not affect the development of DAC, which is guaranteed by the decentralization property.

- Democracy: Changes in the core protocol of the DAC system require voting from vast majority of units, and the decentralization and autonomy feature have determined that the DAC must be a system capable of democratic voting.

Vitalik later extended this idea of DAC and proposed a more general concept: DAO (Decentralized autonomous organization). Unregulated crowd funding and service segregations are components of a DAO, as well as cryptography technological management and trust-based automation. These features allow DAO to run "under the control of a set of business rules without any human participation," just as Stan Larimer said. However, this kind of autonomous organization in ideal state can also lead to serious consequences if there is no strict control during the system design stage. [13].

For example, in June 2016, the DAO, the largest crowdfunding project in the history of Ethereum blockchain, raised more than $150 million USD worth of ETH. Nevertheless, due to the loopholes in code, the organization was attacked by hackers and lost more than 3.6 million ETH, which worth more $60 million USD at that time. Consequently, the ETH community split with the announcement of new security protocols, resulting in the co-existence of two blockchains: ETC and ETH

In the Hcash system, 5% of the coins will be sent to a DAO, and all Hcash holders can determine the use of funds through a real-time dynamic voting system, for example, development of wallets and other infrastructures, or carrying out marketing campaign and other public relation activities. The DAO is the driving force behind future advancement of Hcash community and provides the community with an unfailing supply of vitality. At the same time, the code for Hcash DAO will go through rigorous audits and adds necessary human intervention at the initial stage (Hcash foundation would invite a third party to conduct security audits on the code). This is to protect the DAO from making significant errors in the utilization of funds at early stage.

D. Hidden: Zero Knowledge Proof

Zero Knowledge Proof (ZKP), also known as zk-SNARK, is the core technology behind the anonymous characteristic of Zcash. ZKP allows the prover to convince the verifier that a certain assertion is correct without providing any useful information.

Taking into account the massive amount of data interaction in Hcash, we use an identification scheme where the security is based on the difficulty of solving the discrete logarithm problem. The scheme can be pre-computed to reduce the amount of real-time calculation and the amount of data needs to be transmitted. In order to generate the key pair, first select the parameters of the system: prime p and prime q, where q is the prime factor of p - 1. $p \approx 2^{1024}$, $q > 2160$. Element g is with order q, where $1 \leq g \leq p - 1$. Let a be the generator of GF (p), then $g = a\ (p - 1) / q \bmod q$. The system parameters (p, q, g) and the verification function (that is, the public key of the trusted third-party T) are distributed by T to verify the signature of T on the message.

Give each user a unique identity *I*. User A (with identity *IA*) would select a secret key *s*, $0 \leq s \leq q - 1$, and calculates $v = g - s \bmod p$; A would then send *IA* and *v* reliably to *T* and obtains a certificate from *T*. Let $CA = (IA, v, ST(IA, v))$, where *ST*(.) is the signature generated by *T*.

The protocol is as follows:

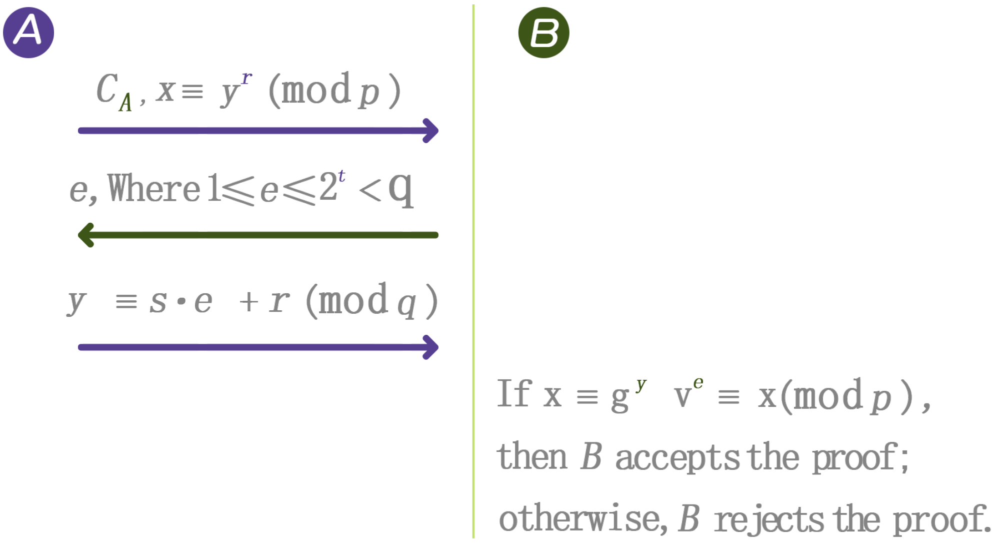
(1) Select the random number r, where $1 \leq r \leq q - 1$. Calculate $x = gr \bmod p$, which is a pre-processing step that can be done before B appears;

(2) A sends (*CA*, *x*) to B;

(3) B solves *ST* (*IA*, *v*) with the public key of *T* and verifies the identity *IA* and public key *v* of A, and send a random number e between 1 and $2t - 1$ to A, where *t* is a security parameter;

(4) A verifies $1 \leq e \leq 2t - 1$, calculates $y = (s\ e + r) \bmod q$, and sends *y* to B;

(5) B verifies $x = gy\ ve \bmod p$. If the equation holds, then it can be recognized that the identity of A is legitimate.


A
B
$C_A, x \equiv y^r \pmod p$
e, Where $1 \leqslant e \leqslant 2^t < q$
$y \equiv s \cdot e + r \pmod q$
If $x \equiv g^y\ v^e \equiv x \pmod p$,
then B accepts the proof;
otherwise, B rejects the proof.

The security is based on the parameter *t*, where *t* is chosen to be large enough so that the probability of guessing e correctly 2^{-t} is small enough. The suggested value for t is 72, and the suggested lengths for *p* (that is, |*p*|) and q (that is, |*q*|) are 512 bits and 140 bits respectively.

This protocol is a zero-knowledge proof of s that does not reveal any useful information about *s* in the verification process.

Hcash will draw from the technique of Zero Knowledge Proof from Zcash. It will not only be used to achieve bi-directional encryption in the process of asset transfer, but also be deployed in many other areas that have high demands on transactional privacy. Hcash has incorporated real-time communication function into the client, which can not only support cross-platform token transfer via a black address but also achieve high privacy in day-to-day peer-to-peer communication through the technique of Zero Knowledge Proof, as well as realizing cross-platform encrypted communication such as from Hcash client to Byteball client and vice versa.

E. Hard: Quantum Resistance

Currently within the blockchain systems represented by Bitcoin, SHA-256 hash calculations and ECDSA elliptic curve cryptography serve as the most basic security protection along the Bitcoin network. However, with the advancement of quantum computer technology, especially within Shaw's algorithm (a typical representative of the quantum algorithm), related operations can be achieved from the index level to the polynomial level in theory. Problems that are difficult for a classical computer in the foreseeable future can certainly be solved by practical quantum computers.

Post-quantum cryptography, also known as quantum-resistant cryptography, is able to resist the attacks by quantum computers. The development of such encryption technology takes a more traditional path, based on difficult problems in specific mathematics fields. Through researching and developing algorithms, the post-quantum secure encryption technology can be applied in the network, and to provide the highest level of data security.

The application of post-quantum cryptography does not rely on any quantum theory phenomenon, but its computational security can defend against any form of quantum attack that is currently known. In 1997, IBM researchers proposed an encryption scheme called Learning With Errors (LWE)[14][15], which means to learn with error. As it takes a long time to find the nearest lattice, it can resist attacks from the quantum computer.

Ring-LWE-based public key encryption scheme: **Related parameter selection and operation rules.**

The main parameters of the program are $\boldsymbol{n}$, $\boldsymbol{p}$, $\boldsymbol{q}$.

n: the maximum number of polynomials in the encryption scheme. In the guarantee of efficiency and security standard, it should be $2k$.

q: a large modulus, which is a positive integer. The value of q is related to the specific case. The q value should be large enough to ensure that the security is high, but the greater the value of q, the more system resources will be consumed and the computation will be increased as well.

p: a small modulus, usually a small positive integer. Let $R = Z\ q[x] /(xn + 1)$, the two polynomial f and g in the ring are expressed as follows $f(x) = f_0 + f_1(x) +... + f_n\text{-}1(xn\text{-}1)$, $g\ (x) = g_0 + g_1(x) + ... + g_{n\text{-}1}(xn\text{-}1)$, $k \in \mathrm{R}$, Define the following operations: $k \cdot f(x) = kf_0 + kf_1(\mathrm{x}) + ...kf_{n\text{-}1}(xn\text{-}1)$

Private Key Generation

$$f(x) \cdot g(x) = \sum_{k=0}^{n-1} \Big(\sum_{i+j=k(modn)} f_i g_j \Big) x^k$$

In this scheme, the encryption public key is $h\ (x)$, the decryption private key is $f\ (x)$ and $fp\ (x)$. The selection method is as follows:

$f(x) \cdot g(x) = 0 \bmod q\ f(x) \cdot fq(x) = 1 \bmod q\ h(x) = fq(x) + 1$

The public key is ($h(x)$, $g(x)$),and the private key is ($f(x)$, $fp(x)$).

Encryption process

In the scheme, the random error polynomial is introduced when encrypting, $e(x) \in \Psi\alpha$, $\Psi\alpha$ is a Gaussian distribution with the parameter α, and the plaintext is converted to the polynomial $m(x)$. The ciphertext is: $c(x) = h(x) \cdot m(x) + g(x) \cdot e(x)$

Decryption process

The received ciphertext is $c\ (x)$, and the steps for decrypting the ciphertext using the private key $f\ (x)$ and $fp\ (x)$ are as follows:

$$\begin{aligned} \alpha(x) &= f(x) \cdot c(x) \\ &= f(x) \cdot h(x) \cdot m(x) + f(x) \cdot g(x) \cdot e(x) \\ &= [f(x) \cdot fq(x) + f(x)\ ] \cdot m(x) + f(x) \cdot g(x) \cdot e(x) \bmod q(1) \\ &= f\ (x) \cdot m\ (x) \end{aligned}$$

$$fp\,(x) \cdot \alpha\,(x) = fp\,(x) \cdot f\,(x) \cdot m\,(x) \bmod p$$
$$= m\,(x)\ (2)$$

In the decryption process of steps (1) and (2), there may be a decryption failure. When the coefficient of step (1) is not in the interval (- q2, q 2) or Step (2) coefficient is not in the interval (- p2, p2), there will be decryption failure. But as long as the selection of the appropriate parameters, the possibility of decryption failure is still very small. We also can be use the algorithm similar to NTRU to avoid decryption failure.

Hcash will develop a Ring-LWE key exchange protocol that works with OpenSSL to achieve post-quantum secure in blockchain.

F. Handy: Limited Blockchain with Unlimited Transaction

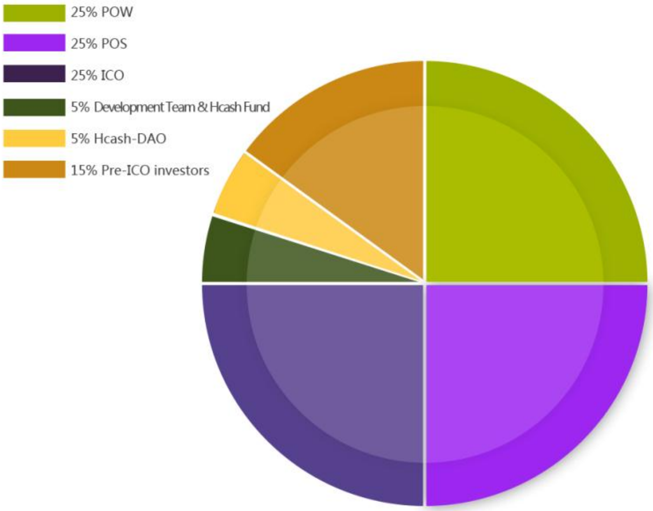
The DAG technology itself is not based on blocks. Therefore, it is not subject to the constraints of block validation time (for example, the validation time for Bitcoin and Ethereum is 10 minutes and15 seconds, respectively). Due to the need to take into consideration the interaction between Hcash and DAG-based blockchain system, the system has incorporated some of the advantages and strengths of DAG in its design. Thus, the validation time for transactions in the Hcash system is almost instantaneous. Also, as DAG is not based on blocks, there is no so-called block size limit in DAG. In theory, the amount of transactions that can be accommodated per unit time is fairly large (HTPS, Hyper Transaction Per Second). At the same time, Hcash needs to account for interaction with block-based blockchain systems. Consequently, it is possible for Hcash to realize a mass number of transactions per unit time under a limited block volume, thereby truly fulfilling the function of "HyperCash".

G. Haven: Limited Token Supply

The total supply of Hcash is fixed. About 84 millions of tokens will be created, and will be distributed through the following six channels:

- 21 million (25%) will be created via PoW;
- 21 million (25%) will be created via PoS;
- 21 million (25%) will be issued for ICO and given to the community for free;
- 12.6 million (15%) will be issued for Pre-ICO sales.

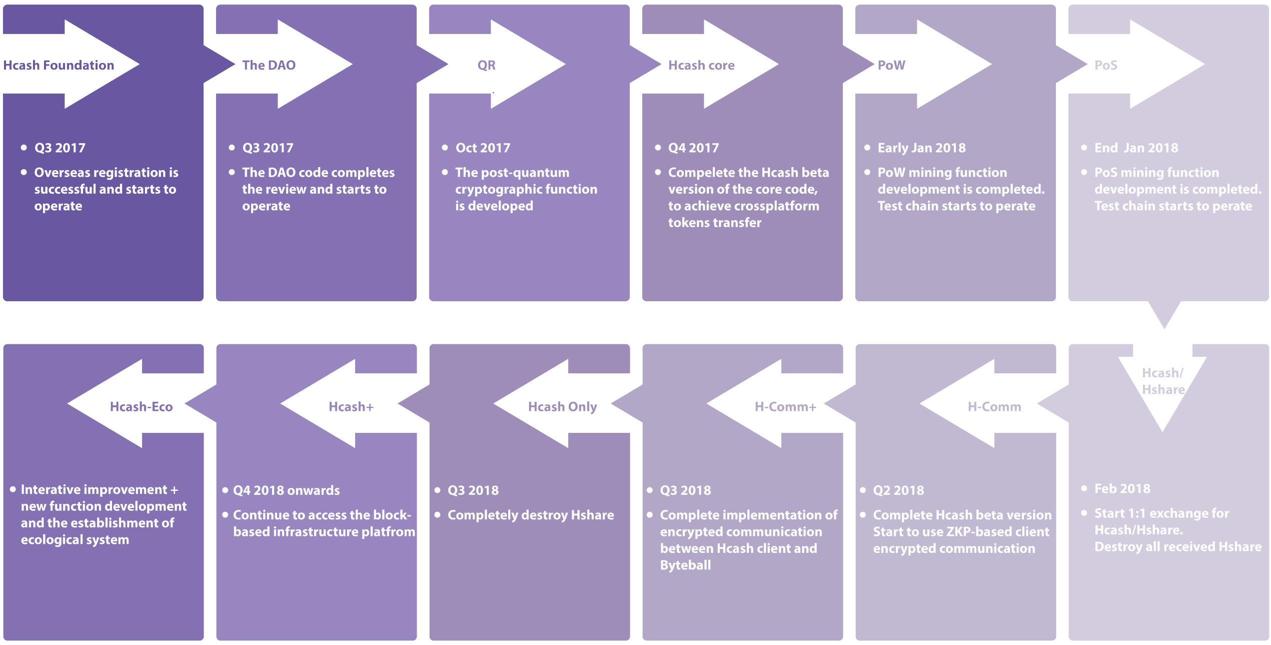
- 4.2 million (5%) will reserved for the development team & Hcash fund,
- 4.2 million (5%) will reserved for Hcash-DAO.



Hcash has both white and black addresses, which corresponds to the transparent address of Zcash and Whitebyte of Byteball, and the Z-Add of Zcash and Blackbyte of Byteball, respectively. Hcash users can convert their white addresses to black addresses or vice versa in their own wallets, provided that the total number of Hcash remains unchanged. In the default definition of the system, the 21 million tokens generated by PoS mechanism will all go to the dark address, and this part of the coins are called HiddenCoins. Similarly, the 21 million tokens generated by PoW mechanism will also go to the dark address as HiddenCoin by default when new blocks are found. Except for the 50% of Hcash above, all of the remaining coins will go to the white address, including the part for ICO and free distribution, early investors, and the coins held by development team and Hcash Foundation and Hcash-DAO. The coins in either white address or black address can be sent upon request during conversion between different systems or transmission between different users.

III. Development Roadmap

As Hcash is focusing on building new technical standards and redefining value, the technical challenges faced by the team are unprecedented. The expected development roadmap for Hcash is shown as below and is only for reference:



Hcash Foundation
- Q3 2017
- Overseas registration is successful and starts to operate

The DAO
- Q3 2017
- The DAO code completes the review and starts to operate

QR
- Oct 2017
- The post-quantum cryptographic function is developed

Hcash core
- Q4 2017
- Compelete the Hcash beta version of the core code, to achieve crossplatform tokens transfer

PoW
- Early Jan 2018
- PoW mining function development is completed. Test chain starts to perate

PoS
- End Jan 2018
- PoS mining function development is completed. Test chain starts to perate

Hcash/ Hshare
- Feb 2018
- Start 1:1 exchange for Hcash/Hshare. Destroy all received Hshare

H-Comm
- Q2 2018
- Complete Hcash beta version Start to use ZKP-based client encrypted communication

H-Comm+
- Q3 2018
- Complete implementation of encrypted communication between Hcash client and Byteball

Hcash Only
- Q3 2018
- Completely destroy Hshare

Hcash+
- Q4 2018 onwards
- Continue to access the block-based infrastructure platfrom

Hcash-Eco
- Interative improvement + new function development and the establishment of ecological system

Hcash and Hshare

Since it takes time to implement Hcash code and develop various features listed above, after the end of the ICO, all the investors will get Hshare first as a sort of placeholder, which is developed based on existing mature UTXO model. After the Hcash main chain is launched, the holders of Hshare can redeem any Hshare they have in any online exchanges or with Hcash official team for Hcash at a rate of 1 Hshare = 1 Hcash. After about 10 months, all redemption and replacement will be completed. At then, the Hcash team will use technical means to destroy all Hshare permanently. Hshare's open source code can be found under Hcash's GitHub page - everyone can read and review the source code and check if the total number of Hshare issued is consistent with the number of Hcash stipulated in the white paper.

IV. Project Risk and Risk Management

A. Regulatory risk

At present, although some governments, such as Japan, hold a positive attitude towards blockchain technology and cryptocurrency and have established favorable policy to support the growth of the industry, there are still many uncertainties in the regulatory level due to conflicts between the decentralized nature of public blockchain and the policies of existing centralized governments. Governments adverse to the proliferation of the use of cryptocurrencies in local commerce could issue laws and regulations deeming the use of cryptocurrencies a regulated activity. For example, in recent weeks, countries such as China and Korea have issued regulations or statements prohibiting token sales, while other countries like the U.S. have sought to bring the sale of tokens within the regulator control of securities offerings. This could result in holders of Hcash being unable to use their coins in the future without further regulatory compliance.

The management team will use the following ways to manage the regulatory risk:

- The team will set up a separate public relation department that will actively communicate with relevant government authorities and industry practitioners, so as to design and carry out its digital asset issuance, trading, blockchain finance, blockchain applications and other business under existing legal framework.

- The operation of Hcash project neither involves transactions using fiat money nor interferes with the exchange between Hcash and fiat money carried out by third party exchanges. Hcash team focused only on technology.

B. Market risk

The ultimate goal of Hcash is to achieve the free flow of value and information within the blockchain ecosystem. However, since the blockchain industry is still in its infancy stage of development, the project will face a variety of market tests in the future.

The operation team will use the following ways to manage the market risk:

- The Hcash operation team will attend industry meetings regularly and hold press release on project progress from time to time to communicate and discuss with relevant developers regarding current market needs and prospects. This can ensure that the project is able to respond to voices of the community and market.

C. Technical risk

The goal of Hcash is to stablish a new set of cross-platform technical standards, which is a very difficult task in terms of technology development. Therefore, the project puts a high demand on top-notch technical talents and requires extensive research involvement and engagement. If these requirements cannot be satisfied, it will definitely affect the progress of the project and even eventually lead to the failure of the whole project.

The operation team will use the following ways to manage the technical risk:

- The operations team will work closely with top domestic and foreign universities and research institutions to build joint laboratories that focus on the development of innovative blockchain technology. The Hcash foundation will also regularly allocate funds to support the construction of Hcash community and carry out in-depth collaboration with other blockchain and crypto communities, so as to ensure that the technical risks of the project are controllable.

D. Financial risk

Financial risk refers to the significant loss of investment raised through ICO and Pre-ICO sale. For example, hackers or other malicious groups or organizations may attempt to interfere with Hcash distribution or Hcash tokens in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing, In addition, the team may not be able to complete the development progress within the schedule because of personnel and financial problems and so on.

The operation team will use the following ways to manage the financial risk:

- All the digital currency raised through ICO or Pre-ICO sale are stored in multi-signature wallet with cold storage and managed by the directors of Hcash Foundation. Using 3/5 multi-signature, the risk of project funds being subject to expropriation and/or theft can be effectively reduced.

V. Disclaimer

This whitepaper has been prepared by Hcash team for the sole purpose of introducing the technical aspects of the Hcash and its associated platform and underlying blockchain protocol. This document does not constitute any offer, solicitation, recommendation or invitation for, or in relation to, the securities of any company described herein.

The whitepaper is not an offering document or prospectus, and is not intended to provide the basis of any investment decision or contract. The information presented in this whitepaper is of a technical engineering nature only, and has not been subject to independent audit, verification or analysis by any professional legal, accounting, engineering or financial advisers. The whitepaper does not purport to include information that a buyer of Hcash might require to form any purchase decision, and, in particular, does not comprehensively address risks of the Hcash, which are numerous and significant.

Hcash (along with its directors, officers and employees), does not assume any liability or responsibility whatsoever for the accuracy or completeness of information contained in this whitepaper, or for correcting any errors herein. Furthermore, should you choose to participate in the ICO or Pre-ICO sale of Hcash, Hcash does not assume any liability or responsibility whatsoever for any loss of market value of Hcash.

The content of this whitepaper is technically challenging and requires a high degree of familiarity with distributed ledger technology in order to comprehend the Hcash and its associated engineering risks.

Recipients of this document are encouraged to seek external advice, and are solely responsible for making their own assessment of the matters herein, including assessment of risks, and consulting their own technical and professional advisers.

VI. Reference

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Buterin, V. (2014). A next-generation smart contract and decentralized application platform.

[3] Wikipedia. Directed acyclic graph. https://en.wikipedia.org/wiki/Directed_acyclic_graph.

[4] Popov, S. (2016). The tangle. Retrieved from https://iota.org/IOTA_Whitepaper.pdf,

[5] Churyumov, A. (2016). Byteball: A Decentralized System for Storage and Transfer of Value. Retrieved from https://byteball.org/Byteball.pdf.

[6] Wikipedia. PoW. https://en.wikipedia.org/wiki/Proof-of-work_system.

[7] Wikipedia. PoS. https://en.wikipedia.org/wiki/Proof-of-stake.

[8] Nxt Community. (2015). Nxt Whitepaper (Blocks). Retrieved from https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf.

[9] mthcl (pseudonymous). (2014). The math of Nxt forging. Retrieved from https://www.docdroid.net/e29h/forging0-5-1.pdf.

[10] Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2.

[11] del Castillo, M. (2016). The DAO Attacked: Code Issue Leads to $60 Million Ether Theft. Retrieved from https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/.

[12] Brafman, O., & Beckstrom, R. A. (2006). *The starfish and the spider: The unstoppable power of leaderless organizations*. Penguin.

[13] Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.

[14] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium* (pp. 267-288). Springer, Berlin, Heidelberg.

[15] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, *60*(6), 43-77.