Hcash

Hcash Whitepaper

HyperCash
The New Standard of Value

Version 0.8.1

30 June. 2017

CONTENTS

Abstract

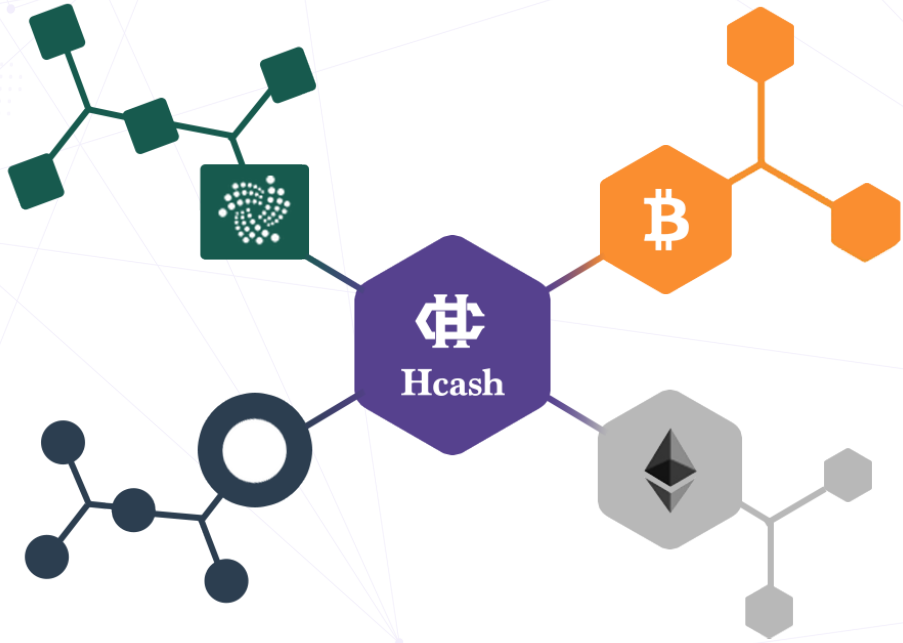
Hcash is the cryptocurrency of a distributed ledger which links both block-based and blockless-based blockchain systems.

The UTXO-based blockchain system (e.g. Bitcoin [1]) and account-based blockchain system (e.g. Ethereum [2]) opened the door of a brand-new world for us. Despite facing some drawbacks along the way, the impressive success of Bitcoin and Ethereum has certainly proven the value of the blockchain technology and its massive potential in the future. Since 2015, there has been quite a few highly-promising distributed ledger systems which are not block-based blockchain technology turned up, 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 fundamental currency in block-based blockchain system. IOTA [4] or Byteball [5], on the other hand may fulfil a similar role in a system based upon DAG. Although all blockchain issued tokens can be traded on some exchange platform, they can only be circulate within its own blockchain system. We want to create a new decentralized platform, which will be the connecting point for all the blockchain system, regardless whether they are block-based or blockless-based blockchain systems, hence allowing value and information being circulated freely between different blockchain system. We call it “HyperCash” or Hcash in short.

1. Introduction

Hcash will create an all new platform that links to major blockchains, allowing value and information to circulate between the different blockchains, hence redefine the value of blockchain. Below are some important features of the Hcash platform.

1.1 Hive. Composed of Blockchain and DAG systems

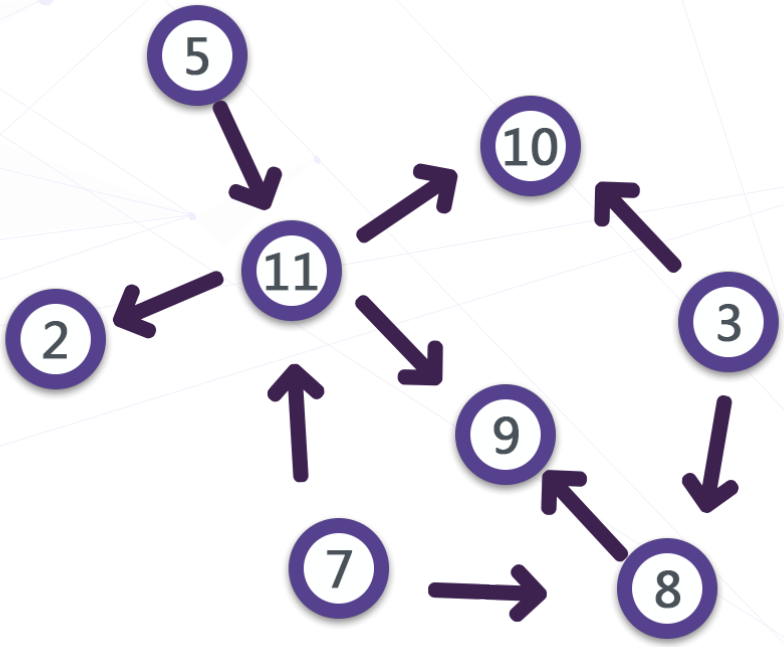


Blockchain-Based *Blockless-Based*

Hcash platform is designed to be the side chain for both block-based and blockless-based blockchains. Hcash will be the value and information carrier for all blockchains to enable the exchange of value and information possible for between the systems.

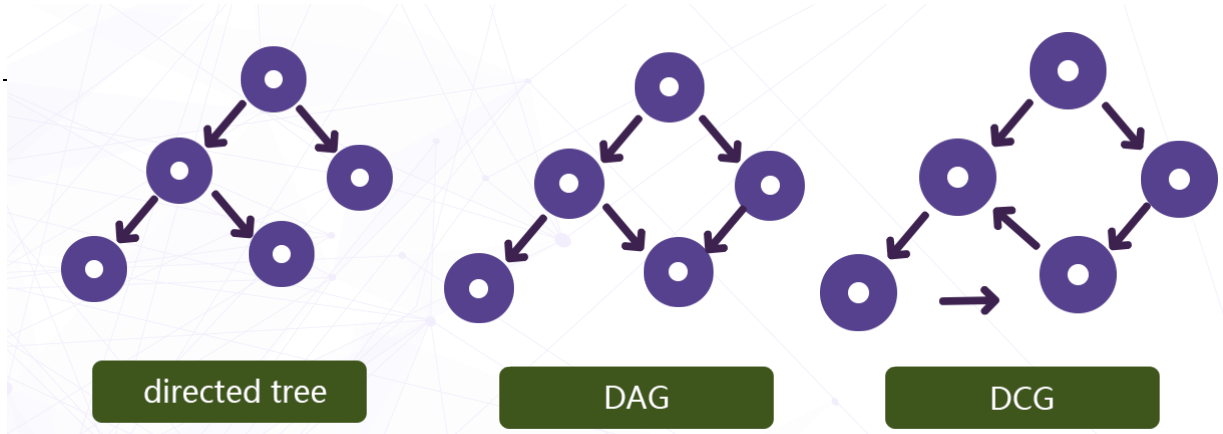
Address Definition

In order to implement with another important feature which we will mention later, Hcash is designed purposely have both public and private addresses to be compatible with Zcash and Byteball address systems. In the near future, it is expected to directly send and receive ZEC or GBYTE in the Hcash system. Meanwhile, it is also possible to achieve the fully encrypted communication based on Zero Knowledge Proof technology between the Hcash nodes and clients, as well as a range of other exciting new features.



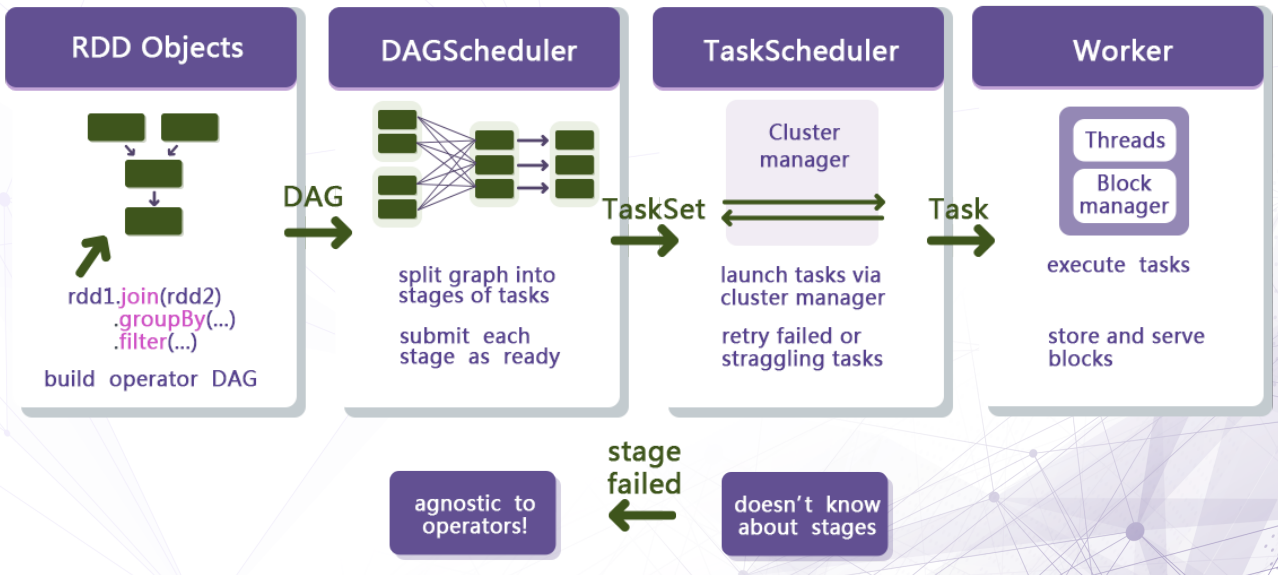
About Directed Acyclic Graph

Directed acyclic graph 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.

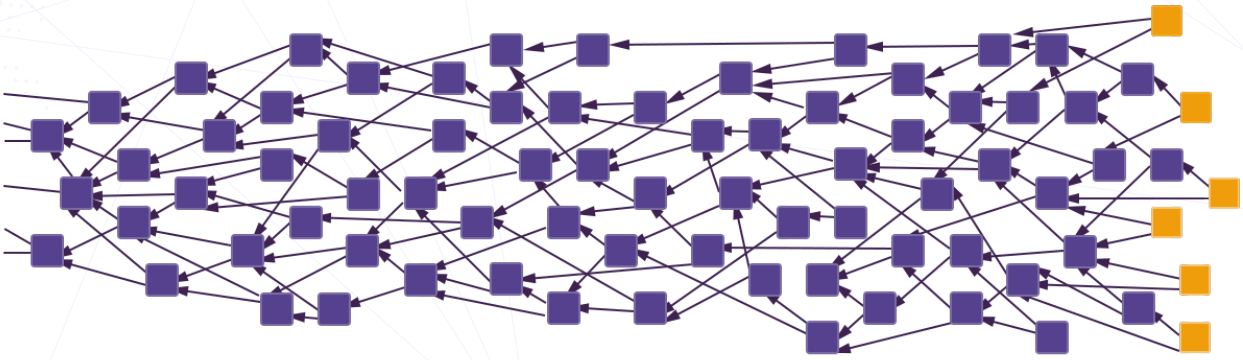


The DAG graph is a special but more general directed graph compares to the directed tree. The following figure shows the examples of directed trees, DAG graph, and directed graph. In the Big Data industry, DAG is usually used for Big Data structural level, such as the execution engine of Hadoop, Storm and Spark.

The following graph shows the operating architecture of Spark:

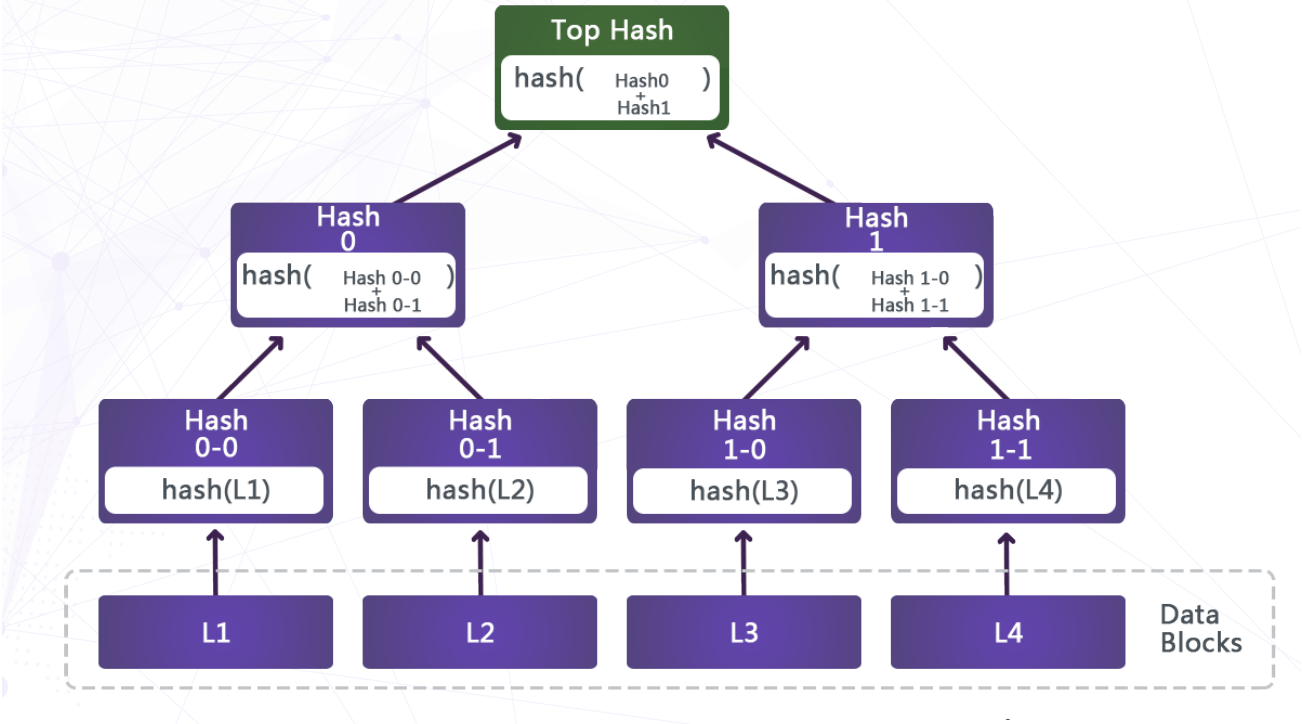


There is a dependent relationship between the RDD objects which forms a DAG situation. The DAG scheduler will split DAG into ‘Stages’. The rules for splitting are simple: scanning through from back to front, whenever DAG scheduler encounters a narrow dependence the current ‘Stage’ will be added in whereas a wide dependence will be split. After completing the division of the ‘Stage’, DAG scheduler generates the ‘TaskSet’ based on each ‘Stage’ and submit the ‘TaskSet’ to ‘TaskScheduler’. ‘TaskScheduler’ is responsible for the specific task scheduling, to



As blockchain technology develop, many new blockchain data structure are now developed base on DAG, for example IOTA [4]. IOTA’s core data structure, called ‘Tangled’, is trying to resolve existing issues in the ‘Internet of Things’ industry such as massive data storage and distributed computing. In addition, it provides a good solution for the micropayment in the IOT industry.

Traditional blockchain such as Bitcoin and Ethereum are using binary tree data structures such as the Merkel tree:



Hcash attempts to establish a channel between the systems, on top of two completely different data structures, so that it can be compatible with the current mainstream blockchain technical standard while allowing the new blockchain technology communicate with the current blockchain system. Hcash's technical development team consists of technical experts from the world's famous academic institution of cryptography and blockchain industry, as well as the experts in Big Data and Cloud Computing. All these expert will ensure the Hcash project meet its original system design goals.

1.2 Hybrid .POW+POS Open-Governance Model

The consensus across digital currency communities has always been a difficult problem to solve. As we all know, the struggle to upgrade the Bitcoin has been affecting the development of the community over the past two to three years. And yet the over-centralisation by Zcash-like digital currencies has certainly deterred active participation across the community.

Hcash, has incorporated partially the philosophy of Decred and Dash, introduces Instant-Open-Governance, which allows all holders to participate in community decisions through the PoS mining mechanism, including protocol updates and upgrades. Hcash is more advanced 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 consensus problem induced from miners, mining farms, exchanges and wallet service providers. The PoW mechanism is set to prevent pre-ICO investors occupying an excessively large portion of rewards in a PoS distribution. It also has been proved to be the most effective security mechanism to protect the blockchain system.

Although an inevitably large amount of energy will be consumed, we believe such setting is still worthwhile in comparison to the security benefits it brings to system. Moreover, it is possible to have the PoW and PoS mining process combined together to ensure the security of the system.

First, we start mining in a traditional PoW way where the miners compete to solve for a cryptographic hard problem. According to this implementation, the blocks being mined do not contain any transactions (they are more like templates), so the winning blocks will only include a header and the miner's reward address. At this moment, the system will switch to PoS. Based on the information of this header, a set of random validators is selected to sign the new block. The higher the number of coins a validator is holding, the higher the probability of being selected. Once the selected validator completes the signature of the block, the template becomes 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 block gets the correct number of signatures. The fee will be assigned to the miner and the validators who participate in the signature of the block.

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

$$F(Nonce) < Target$$

'Nonce' is a random element, 'Target' is the quantization of the qualified block, and the 'Target' of each accounting node is consistent. In addition, successful operation of PoW also requires the cooperation with the following two principles:

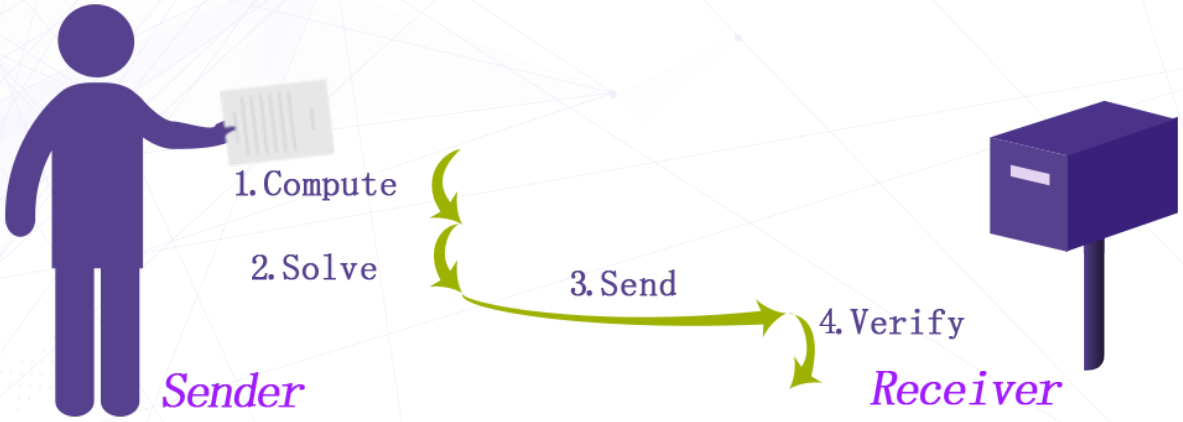
1.Best chain principle: the longest chain is regarded as the right chain.

2.The incentive principle: reward income will be given to those who have found qualified blocks.

Principle 1 is a mandatory rule meaning everyone must obey the rule. The common goal is to find a consistent ledger, and the longest chain represents the greatest workload. If there is no such agreement, everyone will only construct their own chain and no agreement can be reached. Principle 2 is for the workload of incentives. Since it occurs a cost for supporting the network, the only way to encourage people to do so is to provide the incentive according to the workload.

Participation in the accounting blockchain becomes an investment behavior.

The cost, output value, and risk form the game under the constraints of Principle 1, which drive all nodes in accordance with the rules for the real structure of the block, and ultimately to achieve Nash equilibrium.



For PoS [7], the qualifying block can be expressed as:

F(Timestamp) < Target * Balance

The above PoS scheme is currently used by nxt [8] [9] and Blackcoin [10] to take the PoS mechanism. The simplest version of the PoS mechanism can easily lead to a wealth of centralization issues, also has a significant impact on the entire system security. Compared to PoW, the search space on the left side of the formula is changed from ‘Nonce’ to ‘Timestamp’, the ‘Nonce’ range is infinite, while the ‘Timestamp’ is extremely limited. The block time of a qualifying block must be within the specified range of the previous block time, blocks that are too early or too advanced will not be accepted by other nodes.

The target value on the right side of the formula introduces a product factor balance. The larger the balance is, the larger the equation for (Target * Balance) will be this makes it easier for a block to be found. Because ‘Timestamp’ is limited, PoS Casting Block success rate is mainly related to Balance (Stake). Hcash's PoS mechanism will draw on the 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.

1.3 Hierarchy. DAO Governance

The Decentralized Autonomous Organization (DAO) is the ideal product of the cryptography technological revolution. The source 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" portrayed by Yochai Benkler in “Web Fortune” (2006) [12]. But these two concepts are linked with techniques related to cryptocurrencies, and Dan Larimer put forward the concept of a DAC, which regards Bitcoin as a DAC also.

About DAC

In order to have a clear definition of the DAC, we summarize the seven necessary features of the DAC:

- Openness: The design of the DAC system is transparent. Open transparency is the cornerstone of the entire DAC system. A black-box operated organization cannot be treated as a DAC. Nowadays the open source software spirit becomes a typical example of openness.
- Decentralization: No centralized individuals or organizations can control the entire DAC. This feature determines the self-similarity. The decentralization characteristics of the system ensures the vitality of the DAC system.
- Autonomy: Everyone can participate the DAC system. All participants are either DAC system subsidiary or sub-unit, and from their own point of view to promote the development of DAC. The spontaneous behaviour of the participant guarantees the operation of the DAC.
- Value: The DAC system must be of value, such as the international payment network, anonymous transactions, tax avoidance, value storage, non-freezing, unregulated characteristics of the Bitcoin system, which determines the profitability of the Bitcoin DAC system.

- Profitability: DAC participants will receive rewards for DAC system development, and profitability is determined by the value of the DAC itself.
- Self-similarity: Even in the case of only some 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 system of the DAC system require the voting from the overwhelming majority of units to be completed, and the decentralization and autonomy determine that the DAC must be a system capable of democratic voting.

Vitalik extends this concept and brings forward a more common DAO concept. Unregulated crowd funding and service segregations are components of a DAO, as well as cryptography technological management and trust-based automation. Both of which allow the DAO to run, as Stan Larimer said "under the control of a set of business rules without any human participation." However, if there is no strict control during the system design stage. This ideal state of the autonomous organization will also cause serious consequences [13].

In June 2016, The DAO, the largest crowdfunding program in the history, raised more than US$150 million for the distributed autonomous organizations. Nevertheless, due to the code loopholes, it was attacked by hackers and lost more than 3.6 million ETH. At that moment, the value of loss exceeded US$60 million. Consequently, the ETH community split, resulting in the existing ETC and ETH double-stranded coexistence situation.

In the Hcash system, 5% of the coins will be sent to a DAO. Holders of Hcash determine the use of funds in a real-time dynamic voting system, for example, developing wallets and other infrastructure construction, or public promotion and other public relation activities. A DAO is the driving force behind future advancement and provides the Hcash community with continual vitality. At the same time, the code for Hcash DAO will go through rigorous audits and adds the necessary human intervention at the initial stage (by a third party for code security audits). This is to protect DAO in the early stage of fund operation and ensure there will be no major mistake.

1.4 Hidden. Zero Knowledge Proof

Zero Knowledge Proof (ZKP), also known as zk-SNARK, is the core technology behind the anonymous characteristics 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 Hcash data interaction, we use an identification scheme in which its security is based on the hardness 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 required to be transmitted. In order to generate the key pair, we first select the parameters of the system: prime p and prime q, where q is the prime factor of p - 1. p ≈ 21024, q> 2160, element g is with order q, where l ≤ g ≤ p - 1. 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 the message.

Given a unique identity for each user, user A (with identity IA) selects the secret key s, 0 ≤ s ≤ q - 1, and calculates v = g-s mod p; A sends IA and v reliably to T and obtains a certificate from T. We let CA = (IA, v, ST (IA, v)), where ST(.) is the signature generated by T.

The agreement is as follows:

(1) Select the random number r, 1 ≤ r ≤ q - 1, calculate x = gr mod p, which is a pre-processing step that can be done before B appears;

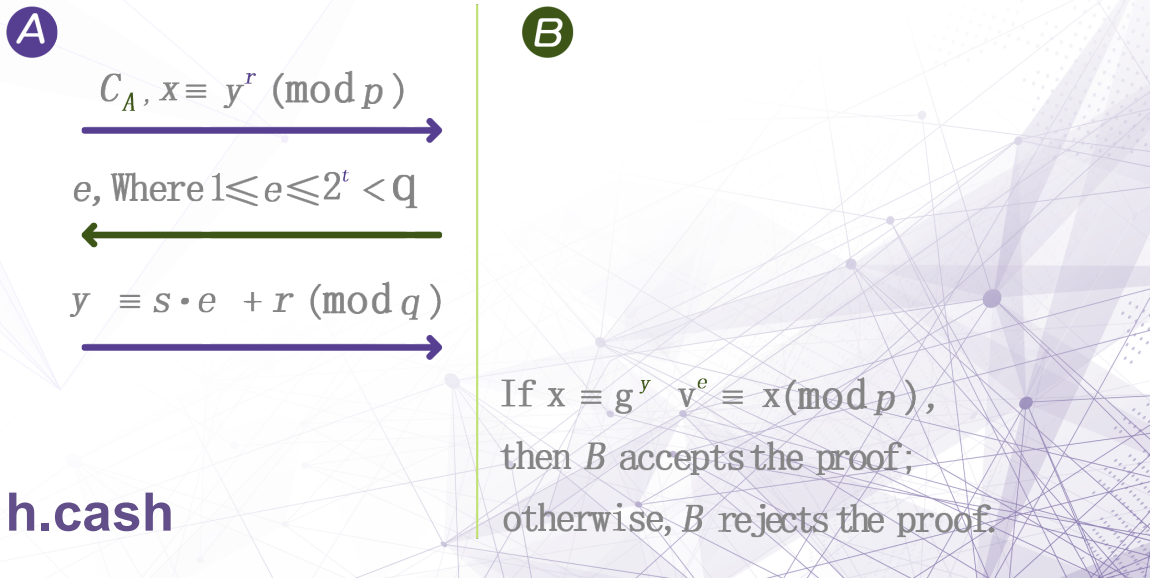
(2) A will send (CA, x) to B;

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

(4) A verifies 1 ≤ e ≤ 2t - 1, calculates y = (s e + r) mod q, and sends y to B;

(5) B verifies x = gy ve mod p, if the equation holds, then recognize the identity of A is legitimate.

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, the suggested length for p (that is, |p|) is about 512 bits, and q (that is, |q|) is 140 bits.



h.cash

Hcash will be motived from the Zero Knowledge Proof technique from Zcash. It will not only be used to achieve bi-directional encryption in the process of asset transfer, but also be deployed to many other areas demanding transactional privacy. Hcash has integrated real-time communication function within the client, which can support multiplatform token transfer via a black address in order to preserve privacy in daily peer to peer communications, through the technique of Zero Knowledge Proof. It further realises multiplatform encrypted communication such as from Hcash client to the Byteball client.

1.5 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 **n, p, 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) = f0 + f1(x) +… + fn－1xn－1，g(x) = g0 + g1(x) + … + fn－1xn－1，k ∈ R，

Define the following operations:

k · f(x) = kf0 + kf1x+ …kfn－1xn－1

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

Private Key Generation

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) ·g(x) = 0 mod q

f(x) ·fq(x) = 1 mod 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:

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

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

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, p 2), 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.

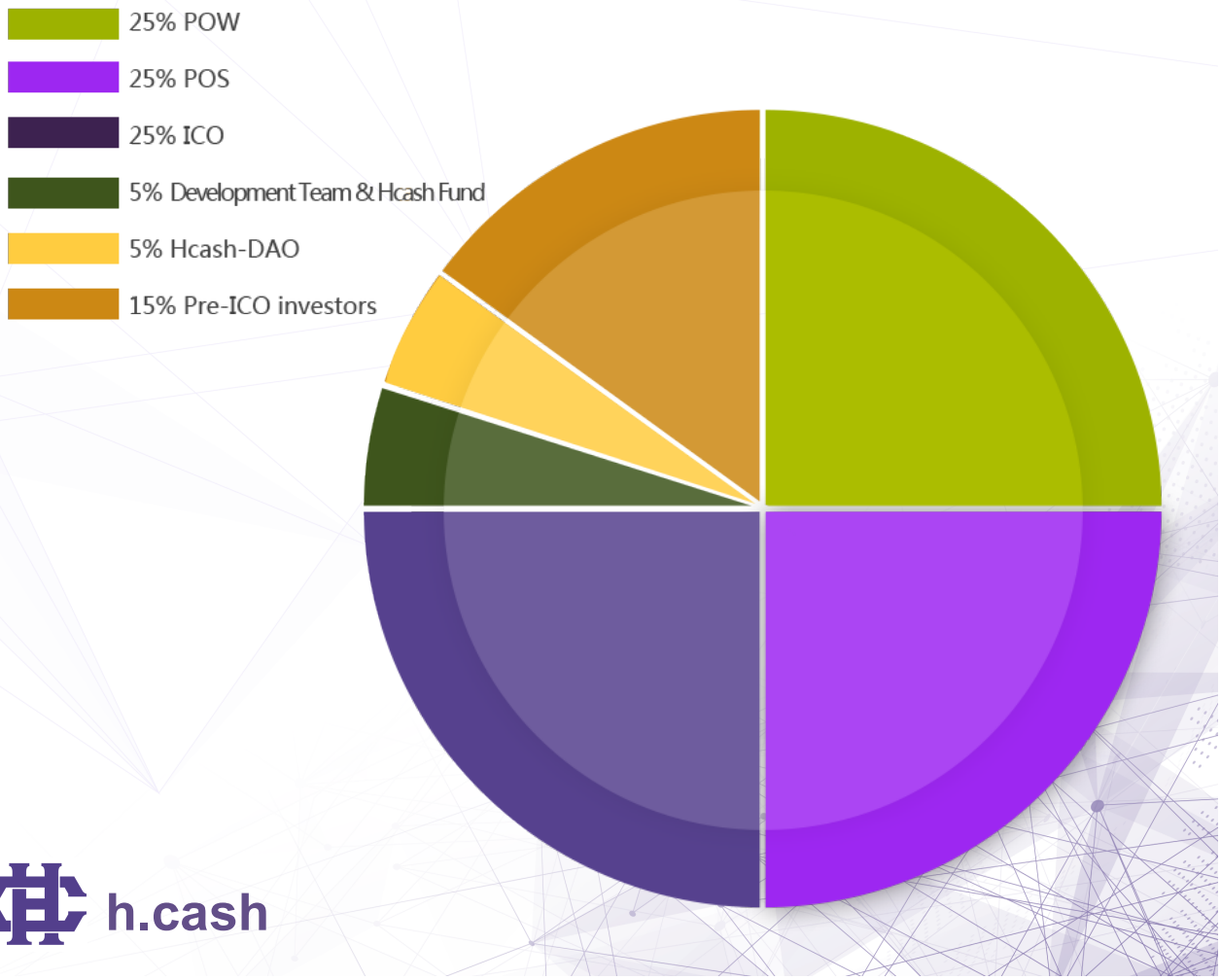
1.6 Handy. Limited Blockchain with Unlimited Transaction

The DAG technology itself is not based on blocks and therefore is not subject to block validation time constraints (for example, the confirmation time for Bitcoin is 10 minutes and for Ethereum is 15 seconds). In its auditing procedure Hcash system is designed to take into consideration the interaction between DAG-based blockchain system thus some of the advantages of DAG will be reflected by Hcash. The confirmation time of the transaction in the Hcash system is almost instantaneous. As DAG is not based on block, there is no so-called block size limit. In theory, the amount of transactions that can be accommodated per unit of time is very large (HTPS, Hyper Transaction Per Second). At the same time, Hcash needs to consider interaction with block-based blockchain systems. Therefore it is possible for Hcash to realize a mass number of transactions per unit time under a limited block volume. That is the real realization of the "HyperCash" function.

1.7 Haven. Limited Token Supply

Hcash has a finite supply of tokens. The supply closes to 84 million, and will be separated into six channels:

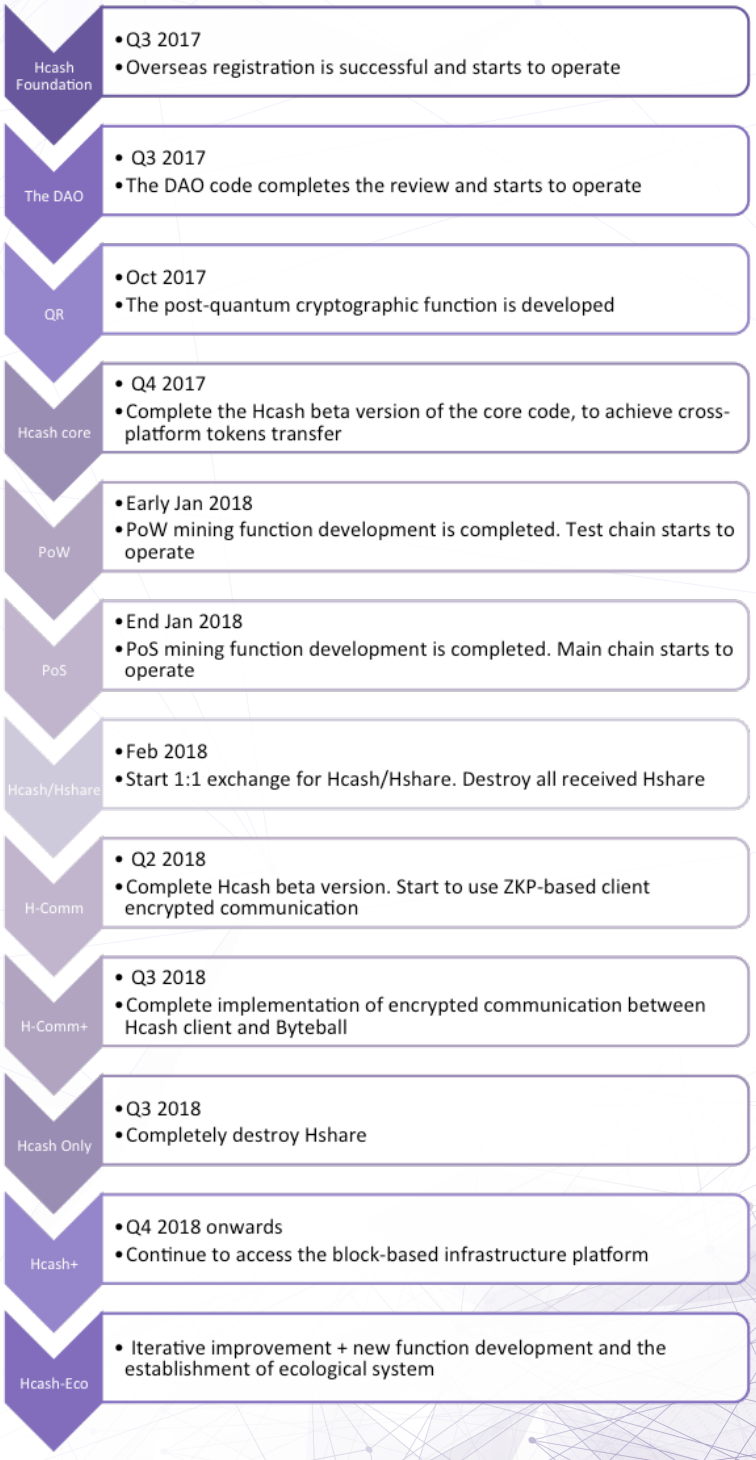
- 21 million (25%) will be created by PoW;
- 21 million (25%) will be created by PoS;
- ICO and free distribution will account for 21 million (25%);
- Pre-ICO investors will hold 12.6 million (15%);
- 4.2 million (5%) will belong to the development team & Hcash fund,
- 4.2 million (5%) will be allocated to Hcash-DAO.



Hcash addresses are divided into white and black addresses, corresponding 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 within their own wallets, provided that the total number of Hcash tokens remains the same. In the system default definition, the 21 million tokens generated by the PoS stream will all go to the dark address. We call this part of the currency Hidden coin. Similarly, the 21 million tokens generated by the PoW stream will also go to the dark address as Hidden coin. For the remaining 50% of the other Hcash, all will go to the white address, including the portion from the ICO and free distribution, early investors, development team and Hcash Foundation holdings and Hcash-DAO. The token can be changed across the two opposite side (white to black or black to white) during the conversion between different systems or transmission between different users.

2. Development Roadmap

As Hcash is focused on building new technical standards and redefining the value, the technical challenges are unprecedented. The expected development roadmap is shown as below:



Hcash and Hshare

Since it takes time to implement Hcash code and feature development, after the end of the ICO all investors will get Hshare which is based on current mature UTXO blockchain as a token first. After the Hcash main line is on the line, you can redeem any Hshare exchange or Hcash official team with Hcash on any on-line Hshare exchange. And after about 10 months to complete all the acceptance and replacement. The Hcash team will use technical means to destroy all Hshare. All Hshare will be permanently destroyed after the deadline. Hshare's open source code Under Hcash's GitHub page, everyone can read and review the source code for Hshare and confirm that the total number of Hsahre releases is the same as the Hcash number specified in the Hcash white paper.

3. Project Risk and Risk Management

3.1 Related risks of Hcash project

Policy risk

At present, although many governments hold a positive attitude and encouragement policy towards blockchain-related industries, there are still many uncertainties due to the decentralization property of public blockchain and the existing centralized government regulations.

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

- The team will set up a separate public relation department, which will actively communicate with the government and industry practitioners, and to cooperate in the legal framework for the design of digital asset issuance / trading / financial blockchain / blockchain applications and related business.
- The Hcash does not involve currency exchange business. But the team will not interfere with third-party exchange to carry out Hcash trading business with existing currency. Hcash team only focus on technology.

Market risk

The ultimate goal of Hcash is to achieve the value of the decentralized free flow in the blockchain system. But since the blockchain industry has just emerged, the future of the project will face a variety of market tests.

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

The Hcash operation team will regularly participate in industry meetings and regularly or occasionally hold project progress and conference to communicate with relevant developers regarding the current market needs and prospects. This can ensure that the project is able to respond to the community and market voices.

Technical risk

Hcash will establish a cross-platform new technical standard, which is a very difficult task in terms of technology development. Therefore, it requires top technical talents and large research involvement. If the control is not good, it will definitely affect the progress of the project and even eventually lead to the failure of the project.

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

Closely rely on the top domestic and foreign universities and the blockchain community, and to build blockchain technology innovation joint laboratories with top universities. The Foundation will also regularly allocate funds to support the Hcash community and collaborates with other blockchain communities to ensure that the project technical risks can be controlled.

Financial risk

Financial risk refers to the significant loss of project fund, such as: fund stolen, development progress incompletion within the scheduled time because of personnel and financial problems and so on.

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

All large amount of digital currency storage are multi-signature wallet + cold storage by the Foundation directors. In the 3/5 multi-signature mode, we can effectively reduce the risks of fund stolen and privately misappropriation.

4. Disclaimer

- This document is used only to convey the purpose of the information and does not constitute a relevant opinion for the sale of Hcash / Hshare. The above Information or analysis does not constitute investment decisions. This document does not constitute any investment advice, investment intention or abetting investment.
- This document does not constitute and conduct of any sale or sale of any form of securities, nor is it any form of contract or promise.
- The investor needs to have a clear understanding of the risks of Hcash, and once the investor participates in the investment, he understands and accepts the risks. The investor is willing to take on all the corresponding results or consequences for this purpose.
- The Hcash team will not obey any direct or indirect losses incurred in participating in the Hcash project.

5. Reference

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Oct 2008

[2] Vitalik Buterin. Ethereum White Paper : A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper.

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

[4] Serguei Popov for Jinn Labs. The tangle. https://iota.org/IOTA_Whitepaper.pdf, April 2016.

[5] Anton Churyumov. Byteball: A Decentralized System for Storage and Transfer of Value. https://byteball.org/Byteball.pdf, September2016.

[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 Whitepaper (Blocks)". nxtwiki. Retrieved 2 January 2015.

[9] mthcl (pseudonymous). "The math of Nxt forging" (PDF). pdf on docdroid.net. Retrieved 22 December 2014.

[10] Vasin, Pavel. "BlackCoin's Proof-of-Stake Protocol v2"

[11] Ori Brafman. The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. 2006.

[12] Yochai Benkler. Wealth of networks: How Social Productions Transforms Markets and Freedom. 2006.

[13] http://www.8btc.com/dao-attack-lost-60-million

[14] Hoffstein J, Pipher J, Silverman JH. NTRU: A ring — based public key cryptosystem

[15] Lyubashevsky V., Peiker T C, Regev O. On ideal lattice and learning with errors over rings