DarmaCash (DMCH) Blockchain

Anonymous, high-performance, extensible blockchain decentralized financial solution

Project White Paper

Preface

Utopia originally means "an imagined place" or "a perfect place", and it can also refer to the state of things in which everything is perfect. DarmaCash (DMCH) is a real financial world that is based on privacy and can create smart contracts to issue privacy stable coins. Through atomic exchange and Oracle, the value exchange between privacy stable coins and DMCH is realized, which allows a value exchange between a new financial world and the real world. We call this - DMCH Utopia.

Contents

Chapter 1 – Introduction 4

1.1 Project background 4

1.2 Project significance 5

1.3 Implementation Method 5

Chapter 2 – Technical Solution 6

2.1 LibP2P 7

2.2 Block-DAG 7

2.2.1 Block-DAG Concept 9

2.2.2 Block-DAG Sorting 11

2.3 Anonymity Technology 14

2.3.1 Ring Signature 14

2.3.2 One-time Key 14

2.3.3 Achieving Anonymity 15

2.3.4 Sub-address 15

2.3.5 Optimization of Anonymity Technology 15

2.4 Consensus Mechanism 15

2.4.1 Problems of PoW Consensus Mechanism 16

2.4.2 PoW+PPoS 17

2.5 Smart Contracts 17

2.5.1 Overview of Smart Contracts 18

2.5.2 DMCH Anonymous Smart Contracts 19

2.5.3 Adaptation of UTXO model of DMCH to Ethereum account model 20

2.5.4 Design of DMCH Anonymous Smart Contracts 21

2.5.5 Dmni Solution Based on Bitcoin Omni 22

2.5.6 DRC-20 Solution 22

2.6 Other 23

Chapter 3 – Core Ecology of DMCH Project 24

3.1 DarmaCash (DMCH) Financial Platform 24

3.1.1 Problems of Centralized Finance (CeFi) 24

3.1.2 Decentralized Finance (DeFi) of DarmaCash (DMCH) 25
3.1.3 Design Logic of DeFi/DEX 26
3.1.4 Ethereum-based DMSwap 26
3.1.4.1 DMS 27
3.1.4.2 DMCHE 27
3.2 DarmaCash (DMCH) Instant Messaging Ecology 27
3.3 DarmaCash (DMCH) Distributed Private Network Ecology 28
Chapter 4 – Token Release Mechanism 29
4.1 Specifications 29
4.2 Mining release 29
4.3 Releasing Curve 29
4.4 Release Principle 29
Chapter 5 – Roadmap 30

Chapter 1 – Introduction

1.1 Project background

Since Satoshi Nakamoto issued the Bitcoin white paper, Bitcoin has laid down principles for the entire blockchain world: *Secure, transparent, and decentralized. All the rules are operated on the blockchain, and no one can do evil things or make unauthorized changes to the rules. All the laws are run by machines and without any human intervention*. The principles of the blockchain give us the image of utopia, which is not so far away from us.

ByteCoin and Monero, based on the CryptoNote protocol, have largely solved the anonymity issue in the Bitcoin payment system. However, in addition to a decentralized payment system, the world also needs more complex decentralized anonymous applications. Unfortunately, due to a low throughput rate, a long waiting time, unsupported smart contracts, Oracle and other issues, Bytecoin and Monero have hindered further development of decentralized applications. For the sake of decentralization, the above problems can only be thoroughly addressed by changing the global consensus, and the cost of which has far exceeded developing a new project.

Besides, in contemporary society, our destiny is manipulated in the hands of others, and most people haven’t realized the fact yet, and even if they have, they are unable to break free. A cashless society is coming without any prior notice, and mobile payment has become more and more common. While people are enjoying the convenience it brings, they have fallen under a more serious surveillance. In the future, paper money and cash may be phased out, as they are not easy for circulation and supervision. A cashless society, featuring a strong circulation and tighter regulation is slowly replacing the old cash flow world.

But it is a nightmare for privacy, as you will live in a world like the one in the movie *the Truman Show*. From the moment you were born, money will be the main theme of your life, such as your food, clothing, housing, and transportation, and thus you are closely monitored because of every penny you spent. The big data will sort out your hobbies, and provide feedbacks to you via commercial advertisements, so as to keep cultivating your hobbies. As the personal privacy data is stored on a centralized server, privacy disclosure is becoming more and more frequent. Centralized bureaucratic organizations can suspend your right to use your money at any time. How horrible it is! And under the money-oriented rules, people will be deprived of privacy and become more and more transparent, and even the basic individual human rights could be compromised.

1.2 Project significance

Internet application services, based on a centralized architecture (including financial services), constantly collect various kinds of user information for different reasons to seek business expansion, but they are oblivious of the protection of users' privacy, which is a basic work, even though it can't boost the growth of profits. However, once the users' information is leaked via such application services, the benefits of hundreds of millions of users will be compromised. The leaked information, if misused by hackers, will bring unpredictable disasters to the users, for instance money or identity fraud.

Nowadays, the society is in urgent need for privacy protection measures that are dominant by technologies and are independent of human will, as privacy is the most basic human right.

The DMCH blockchain project aims to provide an anonymous, high-performance, and extensible blockchain decentralized financial solution that is based on Monero. DarmaCash (DMCH) has adopted the Block-DAG block structure, integrated private addresses, anonymous smart contracts, DeFi, and DEX on the privacy framework of Monero, and introduced decentralized distributed PPoS that is not restricted by nodes. Besides, it also aims to realize a high-speed anonymous global SDWAN by expanding PPoS nodes, and to establish a decentralized distributed anonymous community ecosystem. DarmaCash (DMCH) has not only inherited Monero as an encrypted currency, but also plans to be a decentralized dedicated Internet to protect personal privacy.

1.3 Implementation Method

After over ten years of development in the blockchain industry, tens of thousands of projects have emerged, and most of which have been improved and optimized on the basis of Bitcoin, Bytecoin and Ethereum, and have gradually formed a spiraling evolutionary system. The team members of DarmaCash (DMCH) blockchain project are from different fields, such as cryptography, economics, computer science, and software engineering, and they are committed to protecting privacy under the guidance of the two cycles – *"learning, research, integration and optimization" and "market, demand and fund"*, so as to further integrate and improve the blockchain technology that has been existed for ten years, and eventually to provide the community with a concrete practice of an anonymous, high-performance, extensible blockchain decentralized financial solution. The goal of the DarmaCash (DMCH) blockchain project is to form a monopoly advantage in a specific field, and to constantly strive for and make innovation for achieving decentralization.

Chapter 2 – Technical Solution

At present, the basic structural decomposition of the core module in a blockchain project is shown in Figure 2.1. The whole system has become relatively mature. Continuous operation of the system and constantly emerging business requirements will push forward the unceasing iteration of the blockchain technology. Besides, phenomenal changes will occur in the iteration due to the subversive technological progress (such as quantum computing, hardware breakthroughs, etc.) However, technological updates will not change the framework of the blockchain technology. It will only optimize the core modules under the framework. Therefore, the structure of the anonymous, high-performance, and extensible blockchain decentralized financial solution, deployed under the framework of the blockchain system, is rather stable. As the basic blockchain of decentralized anonymous system solutions, the DMCH blockchain project will continue to integrate the advantages of other projects in the industry, be updated with the latest technology, and optimize its own system on this basis to ensure the stability, advancement and practicality of the blockchain.

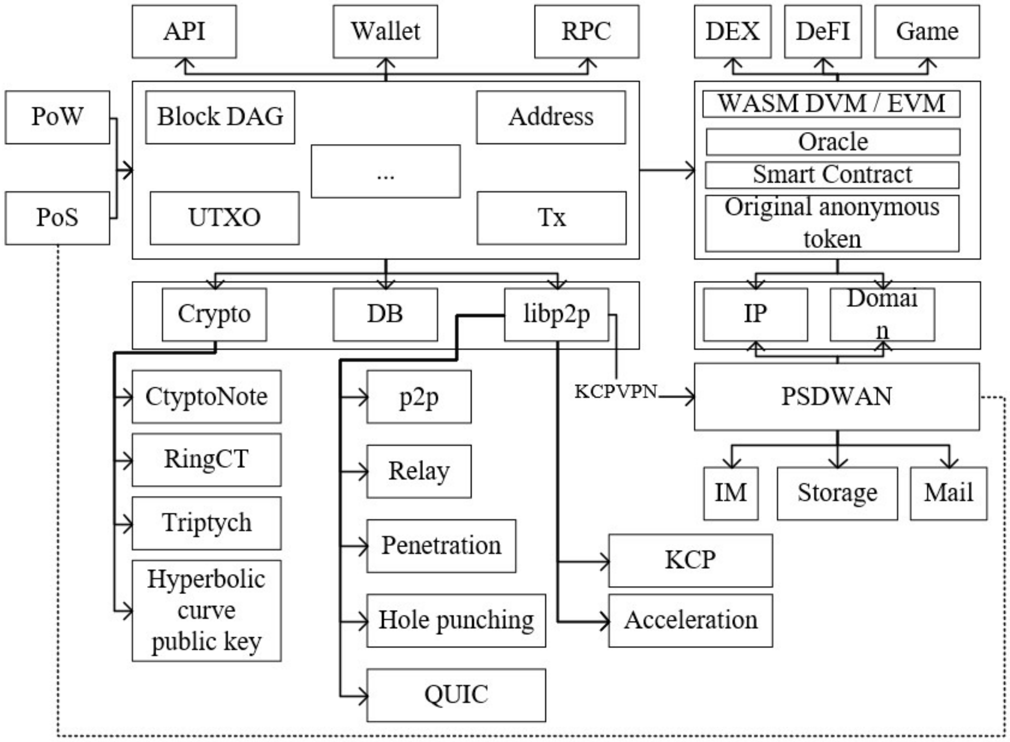

Figure 2.1 System Chart of DMCH Bockchain Project

2.1 LibP2P

The idea of blockchain decentralization has taken root in the general public. In fact, blockchains are just a distributed peer-to-peer (P2P) decentralized network. Many people don't have a clear idea about P2P. P2P network is actually a network in which participants (nodes) can communicate with each other directly and fairly. But this doesn't mean every node is identical, as some nodes play a different role in the network. However, one of the main features of P2P network is that they don't need a privileged "server" that has different "client-side" behaviors, such as the client/server model. The definition of P2P network is very wide, so many different types of systems have been established, and all of which are "equal". The most popular ones are the file sharing networks like BitTorrent, while blockchain networks like Bitcoin, Ethereum and DMCH are also P2P networks.

However, the current Internet is quite fragile, and there are lots of problems, most of which stem from location addressing, but they can be resolved by content addressing, a more flexible distributed peer-to-peer network model. But to achieve content addressing, there are many obstructions from the traditional Internet, which are mainly reflected in various factors such as NAT, firewalls, network delays, network reliability, roaming, supervision, different standards in different devices, and slow technological iterations.

The P2P module of DarmaCash blockchain project will use the LibP2P framework to solve the above problems. LibP2P was originally the network layer of the Protocol Lab IPFS project, but later became an independent project due to its ability to transform the traditional Internet framework.

Simply put, LibP2P is a database that links the nodes with each other. Any two nodes can be connected by LibP2P as long as they have the possibility of being physically linked, regardless of where they are, what environment they are in, what operating system they are running in, or whether they are behind NAT or not. Besides, it is worth mentioning that the QUIC adopted by LibP2P may not be able to achieve global network penetration. DMCH will integrate KCP technology, which has been widely used around the world, and the blockchain internet based on KCPVPN+BGP routing is an important part in the ecology of the anonymous, high-performance, scalable blockchain decentralized financial solutions of DMCH.

2.2 Block-DAG

Blockchain, in essence, is like an account book. It contains information about transactions between all parties concerned, just like any other database. However, if you want the database to be immutable to attacks and – most importantly – maintain the same state on different devices at the same time, it will be tough.

Traditional financial payment systems can process thousands to tens of thousands of transactions every second. By contrast, the transaction processing performance of Bitcoin differs by several orders of magnitude. The transaction processing performance of various well-known blockchain projects is shown in the table 2-1 below:

Table 2-1 Transaction processing performance of different blockchain projects

Name	TPS	Block time
BTC	7	10min
BCH	24	10min
LTC	7~28	2.5min
ETH	20~40	15s

Note: The above data comes from public data on the Internet

Bitcoin adopts the well-known chain structure to organize blocks, and the transactions that each block can contain are limited. When there are several miners working on a block, and several blocks are found at the same time, the miners need to select a "best chain" based on the longest chain principle and temporarily discard the other blocks. The reason why it is "temporary" is because the discarded block will continue to extend and meet the longest chain principle, and then take the place of the former best chain. At the top of the blockchain, the constant “selection, discarding, and convergence” process is called the "selection of the best chain". For example, there are 10 miners who have mined 10 blocks at the same level and at the same time, and in each block, there are 100 transactions, then only one block will be extended on the best chain, while the remaining 9 blocks will be discarded. Therefore, the 900 discarded transactions will be packaged and confirmed in the following blocks. So yes, if all of the 10 blocks can be confirmed at the same time, the processing performance will be increased by 10 times.

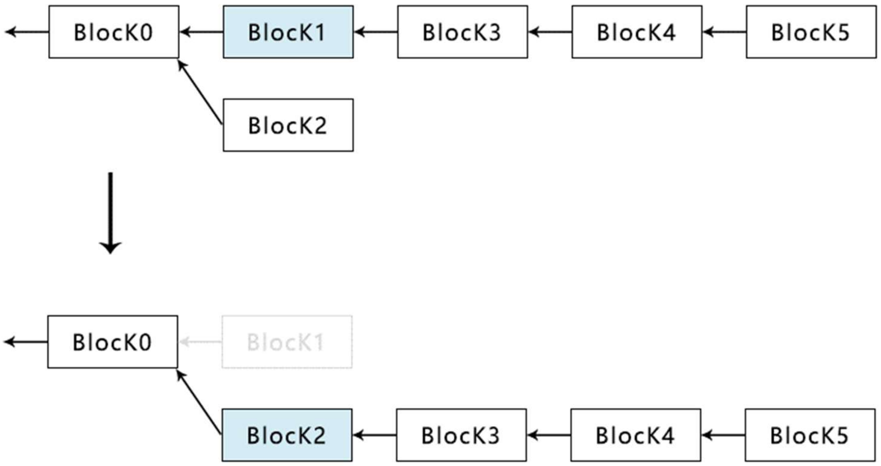

Figure 2.2: Best chain selection of Bitcoin

Choosing the best chain will also bring another important security issue: 51% hash-rate attack. As mentioned earlier, miners who have control over hash-rate can actually manipulate the selection of the "best chain", and overwrite the previous block with their handpicked constructed blocks. So how to prevent 51% hash-rate attack and improve the security of the blockchain has become a hot topic in Bitcoin.

2.2.1 Block-DAG Concept

Block-DAG uses a Directed Acyclic Graph (DAG) to organize blocks. DAG refers to a directed graph without loops. In a non-directed acyclic graph, if a line goes from point A to B via C, and then back to A, then a loop is formed. After changing the edge direction from "C to A" to "A to C", it becomes a directed acyclic graph again. In other words, Block-DAG uses a "graph" instead of a "chain" to organize blocks, and thus fundamentally avoiding the performance and security issues of Bitcoin's "best chain selection". To put it simple, the difference between Block-DAG and traditional Bitcoin is *"Bitcoin's block processing is single-core and single-threaded, while Block-DAG is multi-core and multi-threaded."*

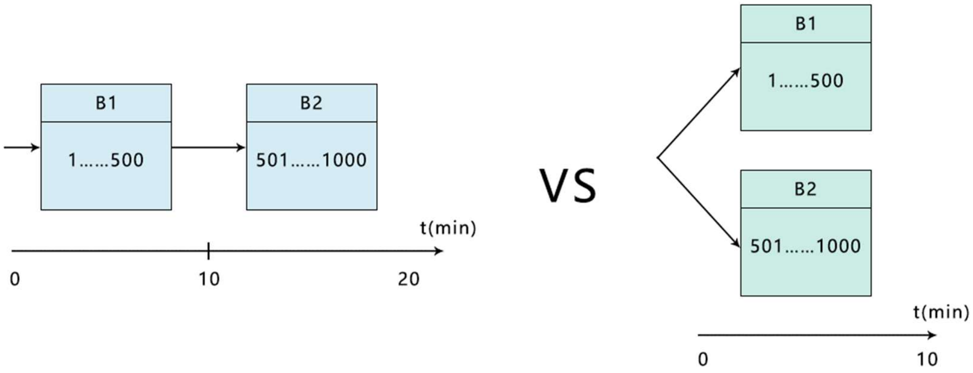

Figure 2.3: Concurrent processing of transactions

Blockchains that are based on Block-DAG are no longer a single chain structure. The entire block forms a network, as shown in the following figure:

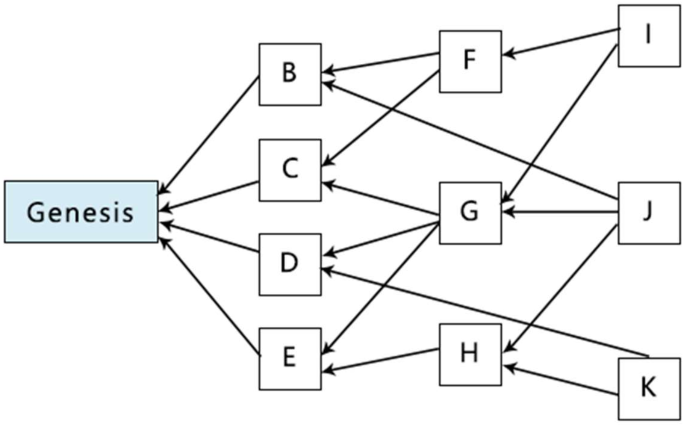

Figure 2.4: Block organization of Block-DAG

As we all know, in a blockchain, blocks are constantly extended to a higher level. In Block-DAG, if a block does not have a new block linked to it, that means the block is at the "top" position, and such blocks are called "Tip". Starting from each Tip, genesis blocks can be traced through only one direction. Tip will be referenced by a new block, and a new block can reference several Tips at the same time. With the aid of the above figure, let's take a look at how the Block-DAG block extends itself:

(1) At the very beginning, the entire blockchain has only one block – the “genesis block”, which means there is only 1 tip. Assuming that there’re 4 miners mining at the same time, 4 blocks {B, C, D, E} will be extended on the same tip.

(2) Suppose that due to mining speed and network transmission, Miner A and Miner B have got {B, C}, Miner C has got {C, D, E}, and Miner D has only got {E} that he discovered all by himself. In this way, they continue to mine on the basis of Tip {B, C}, {C, D, E}, and {E}. They don't need to continue to wait until all node blocks to be consistent, or select the best chain from {B, C, D, E}.

(3) Divide Tip {B, C, D, E} into three groups: {B, C}, {C, D, E}, {E}, which produces new blocks {F, H, I}, and the miners use them as Tip and continue to mine, and the rest can be done in the same way.

In the Block-DAG block, after a tip is utilized by the next block, it is called the "father side", which is similar to the concept of the "father block" in Bitcoin. The "side" is the concept of the DAG algorithm, which will not be further elaborated here. As you can see, due to various unpredictable factors, not every Tip can be a "father side" and continue to extend. This kind of block will be discarded as an “orphan block” in DMCH.

Besides, it is also worth noticing that when a new block appears, how many Tips are allowed to be referenced at best. Considering the most extreme case, if the new block is allowed to reference all the tips it can see, it means that there will be more parallel blocks at the same height, which will bring along the highest transaction processing performance, but the side effects are also very obvious. If there are enough miners, the block will expand without limit. Therefore, we should find a balance for the maximum number of Tips that can be referenced by new blocks. At present, the maximum number of tips that the DMCH allows new blocks to reference is 3. In Version 3 of DMCH, this value can be dynamically adjusted, and, after an integration with transaction shards, it will achieve a huge improvement in TPS.

2.2.2 Block-DAG Sorting

Although it is not a must to sort Block-DAG blocks, in most application scenarios, sorting is very important. This is because in most cases, there is some sort of order-based correlation among transactions. The most typical case is “smart contracts”: the occurrence of a certain condition in one transaction is based on the final executive result of a certain condition in another transaction. Therefore, DMCH needs to "calculate" a "logical sequence" chain in the graphic block according to the algorithm. There are two purposes behind this:

(1) To determine the sequence of transactions, so as to meet the business requirements in the upper level;

(2) To discard orphan blocks; This logical sequence is very similar to the traditional Bitcoin chain structure, but there is also an essential difference between them: Bitcoin implements the sequence through the "Hash of the father block", while the "logical sequence" in DMCH is just a logical concept, and there are no physical connections between the blocks.

The sorted set of blocks is called a "full order". Every block in a full order has only one increasing Topo Height. That is why you can see that there are two heights for each block at the same time on the block browser – Block Height and Topo Height, with the former one being the height of the block on the chain, and it always adds 1 to the Block Height of its largest Tip to ensure that the height of the chain will keep on increasing. Under the same Block-DAG, there may be blocks mined by several miners at the same time.

With regard to the sorting of Block-DAG, many projects or teams have proposed their own solutions. These solutions have their own advantages and disadvantages. Let's see how DMCH is implemented:

(1) After receiving the broadcast of a new block by the miner, the first step is to carry out validity check, using methods such as double-spending detection, transaction validity check, PoW verification, and PoS signature check, etc. Qualified block will be put into the block set.

(2) According to the consensus algorithm, the starting point of the sorting will be found. Suppose “base” is the starting point, then “base” is the genesis block, which will be extended with the development of the blockchain. The block selected to be the “base” is a stable block (without any Side Block, which has been optimized in DMCHv2), and its order will not be changed for sorting in the “full order”.

(3) Starting from “base”, all subsequent block transactions are temporarily marked as invalid.

(4) Retrieve the latest set of tips, with the newly added block included, and the best block is selected as per the consensus algorithm, which is called “best”. DMCH has adopted the "cumulative difficulty sum" to determine the best tip selection. The so-called cumulative difficulty sum is the sum of the difficulty of all the blocks that passes from the genesis block to the current block.

(5) Starting from “best”, tracing backwards to find its tip, and finally obtain all reachable blocks within the range of [“base”, “best”], and afterwards, sort them according to their cumulative difficulty, so as to get the final sorted block set. Obviously, the other tips in the set are not in the [“base”, “best”] range (as they are vertices, and there is no loop in the blocks), and they will be temporarily discarded. Even their father edge, if not referenced by another block, will be discarded at the same time. Temporary abandonment is the normal convergence process in Block-DAG, which will be further elaborated.

(6) Transactions of all blocks in the range will be recalculated according to the sorted block order (Topo Height). Repeated transactions will be automatically marked as invalid. Therefore, double spending is spontaneously avoided, and all transactions have a sequence, which provides basic support for the operation of smart protocols. At the same height, the most difficult block is the main block, and the other blocks are called side blocks.

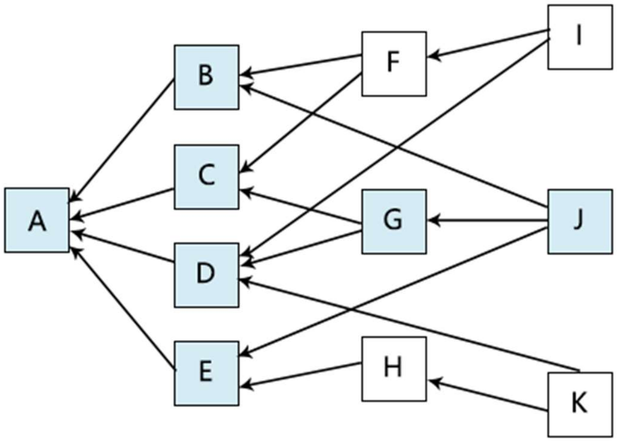

Figure 2.5 Sorting of Block-DAG (1)

As shown in the figure, the candidate tip set is {I, J, K}, and assuming that J is the “best” and A is “base”, the starting point (A has no Side Block), then all the Blocks {A,B,C,D,E,G,J} between [A, J] will be selected and sorted, and {F,I,H,K} will be temporarily discarded.

In the sorting of Block-DAG, there are two points worth noticing:

(1) At the end of Block-DAG, there is always a set of blocks that waits to be converged and sorted. DMCH sets the minimum value of the chain height as 8, and keeps going

forward until the starting point of the “base” is found. DMCHv3 is optimizing the algorithm to reduce the confirmation time. They are “unstable”, because the block may be discarded, and hence resulting in an unreliable transaction, which is very similar to unconfirmed blocks of Bitcoin. In DMCH, the current "stability height" can be obtained through the “getinfo” interface, that means stable and unstable blocks can be distinguished.

(2) As for "temporary abandonment", suppose that the current chain has 10 candidate tips and only one block has been selected, then the remaining 9 blocks may not necessarily be discarded, or at least in most cases this will not happen. That is because the next new block will be selected according to the consensus algorithm when selecting the "father side" (up to 3 selections are allowed at the moment), so when the next new block is selected to be the “best”, they are naturally valid, as they belong to the reachable block in the [“base”, “best”] range. By analogy, the blocks continue to extend backwards, converge and be sorted, and most blocks will be considered valid. As in the above example, once a new block L is generated and {I, J, K} is referenced, all blocks prior to L will also be valid.

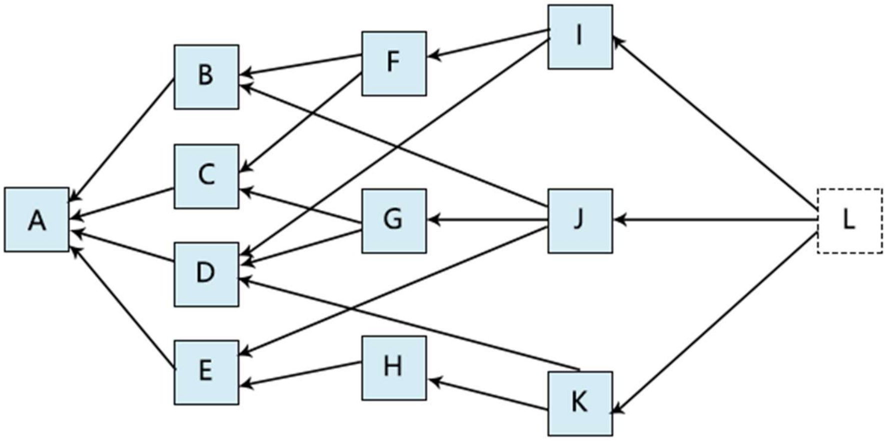

Figure 2.5 Sorting of Block-DAG (2)

Block-DAG is an excellent on-chain expansion solution, which effectively addresses the low processing capabilities in Bitcoin transactions. DMCH's Block-DAG technology is non-conflicting and effectively complementary to other off-chain capacity expansion solutions, such as Lightning Network. Combined with other capacity expansion technologies, DMCH's transaction processing capabilities will be further improved to a great extent. Meanwhile, DMCH's fast and simple block convergence sorting algorithm will also lay a solid foundation for the next smart contract application.

2.3 Anonymity Technology

DMCH is a fork project based on Monero, and both of which are originated from the CryptoNote protocol. The original white paper of CryptoNote appeared in 2012 and was published on Tor. The author of the original white paper used the pseudonym Nicolas Van Saberhagen. In less than a year, after the second edition of the white paper was published under the same pseudonym, the identity of the author still remains unknown. The CryptoNote protocol mainly solves two problems: one is untraceablity, which means that for all incoming transactions, all possible senders may be the source, but it is unknown who sent it; the other problem is unlinkability, which means that it is impossible to prove that any two outbound transactions are sent from the same person. Of course, the CryptoNote protocol can also address other problems. Please refer to https://cryptonote.org/standards/ for more information.

2.3.1 Ring Signature

The non-traceability feature has utilized ring signature technology (Note: this technology can address the anonymity problem of the transaction sender). The ring signature technology is based on the concept of group signature proposed by David Chaum and E.van Heyst (https://www.chaum.com/publications/Group_Signatures.pdf). The ring signature uses multiple public signatures that are mixed together to hide the real signature of the transaction, which will not affect the ability to verify the validity of the transaction.

And it is worth noting that the ring signature technology was later proven to be traceable under certain circumstances (https://eprint.iacr.org/2006/389.pdf). This issue was later addressed by Monero’s Ring Confidential Transactions (RingCTs).

2.3.2 One-time Key

The non-linkable feature has utilized a one-time key technology (Note: this technology can address the anonymity problem of the transaction receiver). Since the public key is required when changing the signature, all incoming transactions of the public key address can be observed on the blockchain, so it is easy to expose all the parties related to the transaction. Therefore, the improved Diffie-Hellman Key Exchange Technology will generate a one-time key to protect all the parties. The general principle is that the sender of the transaction uses its own data to hash the receiver's public key, and thus creating a unique one-time key for the transaction, so only the receiver can generate the private part of the transaction. The CryptoNote protocol is an excellent protocol. For more information, please refer to https://cryptonote.org/inside.

2.3.3 Achieving Anonymity

In the process of achieving anonymity, an individual user has two private keys and two public keys to complete the entire encryption process. Ring Signature technology will guarantee the anonymity of the transaction sender, and one-time address technology (Stealth Address) will guarantee the anonymity of the transaction receiver, and ring confidential transactions (RingCTs) will safeguard the anonymity of the transaction content.

2.3.4 Sub-address

DMCH supports sub-addresses, which is equivalent to the sub-address function of Bitcoin wallets that could pair each address with a set of public and private keys (just like countless "small wallets" in a big wallet file), but DMCH has only one wallet paired with set of public and private keys, which is superior to the Bitcoin solution in terms of performance and maintainability.

2.3.5 Optimization of Anonymity Technology

In order to keep the DMCH anonymity technology in the lead, Monero Research Laboratory (MRL) and the latest encryption technology will be the strong theoretical basis for the continuous optimization of DMCH projects. For example, MRL released Triptych, and proposed ring signatures that are independent of logarithmic size. Unlike MLSAG, Triptych is a new ring signature structure, which integrates MLSAG, Pedersen and Confidential transaction technologies into new RingCTs, so that anonymity can be enforced by more than ten times. The main innovation of Triptych is to make a logarithmic relationship, instead of a linear relationship, between the byte size of the ring signature and the number of decoys. In this way, the ring size can be significantly increased without having major performance issues. The DMCH project will continue to focus on such technological innovations. In terms of Triptych, the DMCH project will be upgraded from MLSAG to CLSAG and eventually transitioned to Triptych.

2.4 Consensus Mechanism

Consensus mechanism can be divided into classic distributed consensus mechanism and blockchain consensus mechanism. The beginning of the research on consensus mechanism can be traced back to 1975 when the "two armies’ problem" was raised in the computer field. Western scholars have researched on the "Byzantine Generals Problem" that centers on how non-faulty nodes can reach a consensus with any specific data when there may be faulty nodes or malicious attacks. The research on consensus mechanism is based on this problem. In 2008, when Satoshi Nakamoto proposed Bitcoin, the consensus mechanism unveiled the blockchain consensus era. At present, the blockchain consensus mechanism can be divided to two categories – one is authorized consensus mechanism and the other is unauthorized consensus mechanism. Authorized consensus mechanism requires the user needs to complete identity authentication before participating in the subsequent consensus mechanism, while under the unauthorized consensus mechanism, which can be represented by Bitcoin, nodes can enter and quit the block chain at any time, and the number of nodes is subject to a dynamic and unpredictable change, and the processes of block producer election, block generation, node verification and blockchain update are carried out through a specific algorithms.

By far, the most successful consensus mechanism is still PoW, namely mining. Basically, all the top 10 blockchains in the industry, with Bitcoin taking the lead, use PoW consensus mechanism. One of the reasons for this phenomenon is that it takes time to form a consensus. When everyone thinks PoW is a reliable consensus mechanism, they'll stick to it, and even if a better consensus mechanism appears, it will take a long while for them to change the new one. The second reason is that PoW has effectively solved the Byzantine Generals problem through encryption methods and economic incentives. Therefore, the fair and decentralized characters of PoW is deeply rooted in the hearts of the general public. Yet, over the ten years since Bitcoin was created, we have to admit that there are some derivative problems occurred in Bitcoin's PoW mechanism.

The blockchain consensus mechanism is mainly evaluated by six aspects, that are – security, transaction throughput, scalability, transaction confirmation time, decentralization and resource occupation. The consensus mechanism of DMCH is formed through three stages – PoW, PoW+PPoS and PPoS. Its transformation pattern follows that of the ETH. Besides, since DMCH is a branch of the Monero project, its security, transaction throughput, scalability and transaction confirmation time have inherited the Monroe's ability. In addition, with the aid of Block-DAG technology and the latest encryption technology, the security (anti-51% double spend attack), throughput capacity (TPS increased to 70), and transaction confirmation time (around 2 minutes) of DMCH has been further improved.

2.4.1 Problems of PoW Consensus Mechanism

So far, PoW consensus mechanism has some disadvantages in resource utilization and decentralization.

(1) Serious waste of resources. Currently, professional machines (ASIC) and lots of electricity are needed for Bitcoin mining, and the electricity it consumes one year is as much as the annual electricity consumption of a small or medium-sized country, and the professional machines that consume the electricity are only doing simple accounting job. Therefore, it is definitely a huge waste of resources to use a country's annual electricity consumption and the corresponding hash-rate to produce bitcoins with highly-fluctuated prices.

(2) Gradual centralization. Satoshi Nakamoto said "one CPU one vote" when he created Bitcoin. But the grand vision has gradually deviated from the course in this

profit-driven society. It can be observed that Bitcoin’s hash-rate around the world has gradually witnessed the monopolization of several large mining pools, and this kind of centralization trend will be more and more serious.

2.4.2 PoW+PPoS

DMCH’s PoW+PPoS refers to the blocks mined by miners that need to be verified by the signature of PoS nodes before they are considered as valid blocks. 5% of the block’s DMCH is awarded to PoW miners and 95% to PoS nodes and token holders. PPoS is an innovation in the DMCH project, meaning distributed PoS nodes. Simply put, unlike the disadvantages of centralized voting caused by EOS super nodes, all the nodes of DMCH are fair, and its mechanism is much more decentralized. The PoW+PPoS phase mainly solves the following problems:

a. Being environmentally-friendly. Since the block reward for miners is only 5%, the incentive mechanism does not encourage PoW mining. This will greatly decrease the input of tremendous calculating resources and electricity, and encourage the supporters to hold and lock coins to earn interests. In this way, the waste of calculating resources and electricity usage can be reduced. That why we call it a real environmentally-friendly mechanism.

b. Being Decentralized. Since 95% of block reward is for PPoS nodes and users who hold and lock coins, people will change their behavior because of the incentive mechanism. Let's make an analogy, Bitcoin’s PoW incentive mechanism forms a “Mining Pool + Mining Machine” ecosystem, while DMCH’s PoW+PPoS incentive mechanism forms a “PPoS Nodes + Hold & Lock Coins” mechanism. In other words, mining Pools have been transformed into PPoS nodes, and mining machines have become hold & lock coins. Can this ecosystem solve the decentralization problem? The answer is yes, and there is a high possibility to form decentralization. First, it is easy to use. The operation of the PoW mining pools and mining machine requires a certain degree of IT technical ability, but PPoS nodes are just a software away. Second, PPoS nodes building incentive mechanism is also effective. Besides receiving rewards when producing blocks (similar to the mining pool fees), there is also collective weight reward available. This means that PPoS node owners will not only receive transaction fees, but also the reward for maintaining the nodes. This will attract more people to build the nodes, which, in turn, helps to make the blockchain more decentralized. Finally, DMCH project can adjust the incentive mechanism based on the decentralization rate, which aims at speeding up the construction of a decentralized network.

2.5 Smart Contracts

Based on WASM, DMCH smart contract uses PLONK zero-knowledge proof, provides a complete C/C++ language and GO language compilation environment, and supports "anonymous" contracts, and is very easy to migrate Ethereum smart contracts to the DMCH smart contract platform.

2.5.1 Overview of Smart Contracts

Smart contracts are an intermediary-free computer transaction protocol that can perform self-verification and automatic execution of contract terms. In recent years, with the increasing popularity of blockchain technology, lots of attention has been paid to smart contracts. Smart contracts on the blockchain are decentralized, trust-free, programmable and unalterable, which can be embedded with various kinds of data and assets to help realize a safe and efficient information exchange, value transfer and asset management. Eventually, it is expected to penetrate into the reform of traditional business models and social production relations, laying the foundation for the construction of programmable assets, systems and society. Usually, there are two properties of smart contract: value and status. “If-Then” and “What-If” statements in the code preset the corresponding trigger occasion and response rules. After the smart contract is mutually agreed by multiple parties, and signed by each party, it is submitted with the user-initiated transaction (Txn), and is transmitted through the P2P network, and stored in a specific block of the blockchain after verification by the miner. The user can invoke the contract by initiating the transaction after receiving the returned contract address and contract interface information. Miners are motivated by the incentive mechanism preset by the system, and will contribute their own hash power to verify transactions. After receiving the contract creation or calling the transaction, the miner will create the contract, or execute the contract code in the local sandbox execution environment (such as EVM). The contract code will automatically judge whether the current situation meets the contract trigger conditions based on trusted external data sources (also known as Oracles) and the inspection information of the world state, to strictly enforce the response rules and update the world state. The transaction is verified before being packaged into a new data block. The new block is authenticated by the consensus algorithm and then linked to the blockchain main chain, and then all updates take effect.

Ethereum has a large developer community, and many cryptocurrency developers are familiar with the Ethereum Virtual Machine (EVM). From the outset, Ethereum has developed Solidity, a language targeting EVM, and used it as the main language for smart contracts. Although Solidity has obvious limitations, compared with common languages such as Go and Rust, it is currently the most widely used development tool on the chain.

Moreover, Web Assembly Virtual Machine (WASM) has been adopted by DMCH, which is an increasingly popular technology in encryption and a broader technical world. Most cryptocurrencies are moving towards this direction, and there are more projects, such as ETH2 and Polkadot, that have decided to use WASM.

Although Web Assembly is bound to be successful, it is necessary to take the transitional adaptation period of developers into consideration, so as to make sure that EVM run on DMCH. Therefore, DarmaCash (DMCH) has integrated the EVM into the

DMCH, and the DMCH will support both the WASM virtual machine and the EVM virtual machine. As most Ethereum tools rely on web3.js, we have implemented a custom-made web3 provider that allows direct communication with Ethereum contracts through familiar interfaces in the web3 library.

2.5.2 DMCH Anonymous Smart Contracts

The development of anonymous smart contracts in the blockchain industry has mainly gone through three stages:

The first stage: Bitcoin is a completely open and transparent blockchain project. You only need to know the address of the wallet to know the income and expenditure of bitcoin. Therefore, it is easy to find out the relationship between different accounts. Associating Bitcoin wallet addresses with real users will make us “transparent”, leaving no room for privacy at all. To solve the bitcoin’s privacy problem, developers have proposed a solution centering on the principle of coin mixing, which involves many people to participate in the transferring (roll-in and roll-out) of Bitcoin, but it is difficult to find a one-to-one mapping relationship between different transfers. Since the roll-in and roll-out are separated, and cannot be traced from one end, user’s privacy can thus be protected.

The second stage: In order to fundamentally solve the privacy problem, some developers have developed blockchain projects that protects privacy from its core. The mainstream blockchains of privacy protection on the market can be divided into four categories: Coin Mixing, Ring Signatures, Zero-Knowledge Proof, and MimbleWimble Series, which are represented by Dash, Monero, Zcash and Grin/Beam respectively. However, these blockchains that focus on privacy protection do not support smart contracts, and can only be used as digital asset tools.

The third stage: After 2018, developers began to realize the growing need for privacy protections in smart contracts, so the privacy layer project began to play an active role in various scenarios. In other words, the intelligent contract on the blockchain provides privacy protection. Note: the privacy layer agreement can be built on the blockchain in the first or second stage. Unlike the blockchain project that protects privacy in the second stage, the privacy layer project can be combined with the system of each blockchain to perform cross-chain operations, which is relatively more flexible, and can meet the specific privacy needs of users and developers. This is the so-called privacy smart contracts.

Currently, well-known privacy smart contract projects based on Ethereum (ETH) include NuCypher, Aztec Protocol and Zether. The anonymous smart contract project based on the Monero (XMR) is DMCH. DMCH has a clear positioning for smart contracts, that is to build an easy-to-use, secure, private, and efficient intelligent contract platform on the basis of Monero, so as to serve the ecological business development of DMCH .

2.5.3 Adaptation of UTXO model of DMCH to Ethereum account model

Ethereum, as a whole, can be regarded as a transaction-based state machine: it originates from a Genesis state, and then as transactions are executed, its state gradually changes to the final state, which is the authoritative version in the Ethereum world. The concept of an “account” has been introduced in Ethereum to replace the Unspent Transaction Output (UTXO) model of Bitcoin, which are divided into external accounts and contract accounts. Both types of accounts have correlated account status and account addresses, and both can store Ether (Ethereum dedicated cryptocurrency). The difference between the two accounts is that the external account is controlled by the user's private key, and there is no code associated with it, while the contract account is controlled by the contract code, and there is a code associated with it.

Users can only initiate transactions in Ethereum through external accounts. The transactions may include binary transaction load data (Payload) and Ether. A series of message calls may be generated during a transaction. When the recipient of a transaction or message call is a specific address Ø of Ethereum, a contract is created. The new contract account address is calculated from the address of the contract creator and the number of transactions (Nounce) issued by the address, and the payload of the contract creation transaction is compiled into EVM bytecode for execution, and the executed output is permanently stored as the contract code. When the recipient is a contract account, the code in the contract account is stimulated for execution in the local EVM. Payload is used as the input parameter of the contract, and the trusted data source provides the necessary external world information for the contract. After all executions are completed, the execution results are returned, and the complete transaction is verified by the miner broadcast and stored in the block chain together with the new world state.

As Ethereum transactions are accompanied by bandwidth consumption, storage consumption, and computing consumption, etc., so in order to encourage the input of global computing power and rationally allocated usage rights, and to prevent the system from going out of control due to malicious programs, the execution of all programs in Ethereum needs to bear a cost. Various operating costs are calculated in “Gas”. Any program fragment can be used to calculate the amount of fuel consumption according to the rules, and the initiator of a complete transaction needs to pay all the execution costs. When the transaction is completed, the remaining fuel will be returned to the transaction sender's account at the purchase price, and the unrefunded fees will be used as a reward for the miner who has mined the transaction block. If out of gas (OOG), stack overflow, invalid instruction or other abnormalities occurs during the transaction execution, the transaction will be invalid, but the consumed gas will still be used as a reward for the miners who have contributed their computing resources.

In order to support the account model of smart contracts, DMCH has introduced the design of "abstract layer for anonymous accounts model”. Due to the existence of the abstract layer, changes for any ordinary UTXO account and smart contract are transparent, i.e. from the perspective of ordinary transactions, the creation and invocation of smart contracts are just a different type of anonymous transaction, which is independent from the account model concept. However, from the perspective of smart contract developers, the account model is used, and the existence of UTXO accounts is not perceptible. Suppose user A wants to transfer money to user C through contract B, then:

(1) User A initiates a contract transaction to the contract address B. The function of the contract transaction is to invoke the transfer function of B, and send the recipient address (usually the sub-address of C) and transfer amount of user C into it;

(2) Upon receipt of the transaction, Contract B executes the contract code, completes the mapping of C's sub-address to the contract account, and triggers the transfer process;

(3) As for the contract accounts, there'll be two transactions: the expenditure of account A and the income of account B, as well as the expenditure of B and the income of C. Afterwards, the contract code will update the balance of the contract account;

(4) After running the contract code, an ordinary transaction to the recipient address C will be triggered automatically.

In this way, from the perspective of the UTXO account model, there are two anonymous transactions, transaction from A to B and transaction from B to C. Yet in smart contracts, there are balance updates in three contract accounts, namely account A, B and C.

Simply put, DMCH maps the sub-address to one contract account, thus completing the transformation from UTXO to account model contract. Therefore, we can see that the operating mechanism of the DMCH smart contract is exactly the same as that of Ethereum.

2.5.4 Design of DMCH Anonymous Smart Contracts

When DMCH implements the account model using sub-address mapping, DMCH smart contracts can actually be understood as Ethereum (ETH) smart contracts. The DMCH project defines the following scenarios in the actual large-scale operation:

(1) The content of the contract is transparent + transparent DRC20-TOKEN (The contract currency of ETH is ERC20, and the contract currency of DMCH is DRC20)

(2) Transparent contract content + anonymous Dmni-TOKEN (Omni has transparent assets on BTC, and Dmni has anonymous assets on DMCH)

(3) Anonymous contract content (achieved via PLONK, and token types do not matter, as they are complete anonymous)

The above three situations have covered most scenarios in smart contract applications. DMCH enables its users to choose the type of smart contract according to the actual situation. In fact, homomorphic encryption (FHE) technology can be used to pursue the anonymity of contract contents, but the current computing power is not capable enough to support the calculation. In most cases, anonymous contracts aim to protect the participants and assets, rather than the whole contract content.

Simply put, the DMCH smart contract is an optional anonymous smart contract. The first "transparent contract content + transparent DRC20-TOKEN" model is exactly the same as the Ethereum contract, i.e. full transparency of all information, which provides the DMCH smart contract with a potentially large user base. The second “contract content transparency + anonymous Dmni-TOKEN” model realizes the protection of participants on the basis of the first model, i.e. the contract assets are protected by the underlying anonymous technology. The third type of "contract content anonymity" realizes the complete anonymity of the contract content. Due to the adoption of Merkel trees and zero-knowledge proof, this contract privacy protection scheme is very computation-intensive, and the gas costs are rather high, and one block cannot accommodate too many transactions of this kind, so it is only used for specific scenarios.

2.5.5 Dmni Solution Based on Bitcoin Omni

Omni protocol is a digital asset solution based on the Bitcoin blockchain (the earliest one is the Master Coin Protocol, as shown in the figure below). The core principle is to attach asset-related operation information (such as asset issuance, money transfer, etc.) to the OP_RETURN information in the Bitcoin protocol. In the native Bitcoin protocol, OP_RETURN information can be arbitrary, and is protected by the Bitcoin blockchain, so it can’t be altered. The Omni protocol layer runs on top of the Bitcoin blockchain, and maintains a local database. The Omni protocol will analyze all the OP_RETURN information in bitcoin transactions, and if the protocol definition is met, the operations are performed, and the asset information recorded in the local database will be updated. Omni protocol is essentially a Colored Coin scheme, and it can be regarded as the most successful colored coin scheme so far. Moreover, the most successful application of the Omni protocol is Omni-USDT.

DMCH has utilized the existing anonymous technology framework (ring signature + one-time address + RingCT) to abstract a set of Omni-like technology framework. It means that you can easily issue your own anonymous digital assets on DMCH without issuing your own main chain or smart contract, and you don’t even need to write a code line.

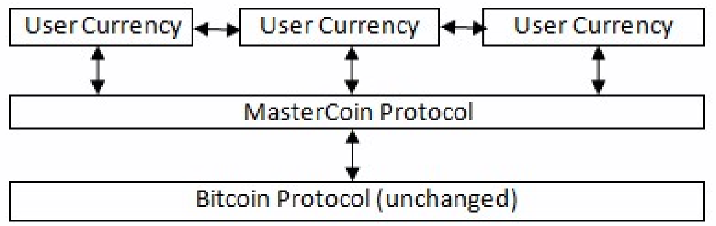

Figure 2.7 Omni Protocol

2.5.6 DRC-20 Solution

DRC-20 Token is a type of DMCH smart contract that complies with the DRC-20 standard. DRC-20 standard defines a series of commonly used interfaces for digital asset operations, which facilitates the implementation of DMCH's C and GO languages (based on WASM). Please note that DRC-20 is just a series of interface definitions and does not contain specific implementations. In other words, digital asset developers need to write their own smart contracts to implement the methods as specified in the DRC-20 standard. Like other general smart contracts, the final execution of DRC-20 Token is essentially a smart contract program running in the DMCH virtual machine (DVM). The DMCH protocol itself does not care about the business logic of the contract, so the performance of a specific DRC-20 Token depends entirely on the programming level of its developer.

2.6 Other

As shown on the system diagram of the technical plan of the DMCH blockchain project in Figure 2.1, the technical plan of the DMCH project is continuously optimized and upgraded according to the principles of two loop iterations – "learning, research, integration, optimization" and "market, demand, capital". There are six aspects of factors for evaluating technology upgrades, namely security, transaction throughput, extensibility, transaction confirmation time, decentralization, and resource occupation. In addition to the above chapters, the technologies that are in the experimental stage include the combination of VRF technology and Block-DAG technology, transition between MLSAG, CLSAG and Triptych technology, as well as database optimization and selection, etc.

Chapter 3 – Core Ecology of DMCH Project

The concrete practice of an anonymous, high-performance, and extensible blockchain decentralized financial solution requires a relatively closed-loop ecosystem (inner loop) and a relatively complete industry ecosystem (outer loop). At present, the decentralized industry ecosystem is relatively complete, and the closed-loop ecosystem is relatively successful on Ethereum. However, the sustainable development of the Ethereum ecosystem has been limited by the technical defects of Ethereum, which affects the continuous and rapid development of the ecology. The closed-loop ecosystem based on DMCH effectively supplements the current situation that the Ethereum ecosystem is insufficient to meet the market demand, while addressing the market's strong demand for privacy and high-performance blockchains.

The DarmaCash (DMCH) blockchain project will build its own core ecosystem of "Instant Messaging IM" and "Distributed Private Network", as well as the DeFi/DEX financial platform, so as to give the community a minimal ecological aggregation that combines financial payments, secure communications and small private networks all in one, and ultimately develop the DMCH ecosystem to even surpass the Ethereum ecosystem.

3.1 DarmaCash (DMCH) Financial Platform

Eighty percent of the world’s wealth is in the hands of twenty percent of the people. This is a social phenomenon that everyone can feel. We call it the "Two-eighth Split" or the "Matthew Effect." The Matthew Effect reflects the polarization of the real society, with the rich becoming richer and the poor getting poorer. The twenty percent is the rule-makers, and the gainers of vested interests. Most people in the world fall into the other 80%, but a majority of them want to be the other 20%. Interestingly though, even if these people have successfully transformed from the lower class into the upper class, the balance will not be broken, as people of the upper class will formulate corresponding rules to protect their own vested interests, that is, the minority group will always be in a dominant position.

The "Matthew Effect" is particularly prominent in the financial world. In the centralized financial world, the power of finance is concentrated, and most people are excluded from obtaining funds, and can only get a small portion of profits from a project. The closed financial world is the shackles that hinder the further development of the economy, as the rules guarantee the interests of a small number of people, and exclude the rest majority.

3.1.1 Problems of Centralized Finance (CeFi)

Centralized financial system is not a healthy financial system. It is just a tool for 20% of the upper class to harvest money from the other 80% of the lower class. The highly concentrated power makes it possible for centralized financial institutions to mark, track and even block your personal assets. Banks are the embodiment of centralized financial institutions. When ordinary people hand over the control of their assets to the banks or trust companies, these financial intermediaries can easily use the money in the market for investment, and when they get high returns, they will give their clients the promised profits. However, financial subprime mortgage crises have frequently occurred throughout the history. Centralized financial institutions couldn’t foresee these risks, and were even more prone to make mistakes. These risks will cause great harm in a centralized system. In the centralized financial world, there are thresholds for the participation of financial events. For example, private equity, venture capital, and financing mergers and acquisitions are all involved with private equity funds or some big shots in the financial market, and ordinary investors can never bridge the capital gap. Therefore, most high-quality project opportunities are controlled by the upper class. Even if you understand thoroughly about the future development of the industry, you may still be shut out due to insufficient capital strength.

3.1.2 Decentralized Finance (DeFi) of DarmaCash (DMCH)

The concepts of “decentralized finance, distributed finance, and programmable finance” that we get to hear more often can be of equal value to DeFi, which has several prominent features:

(1) Based on blockchain technology;

(2) Assets are controlled by individuals;

(3) Clearing and settlement are all done in real time through smart contracts;

(4) The cost of trust between individuals is reduced by minimizing dependence on trust;

Decentralized finance (DeFi) is an open source technology that aims to disintermediate by introducing a decentralized layer, and eliminating the rent-seeking middlemen, so as to improve the current financial system in all aspects. DarmaCash (DMCH) expects that everyone to be their own master, and everyone can schedule their own assets freely, without being spied, supervised, or blocked by centralized institutions. DarmaCash (DMCH) will build a Utopian world of DarmaCash (DMCH) on the basis of decentralization, privacy and fairness, so as to ensure financial security and the fairness of each investor’s financial participation, to fight against asset review and supervision in the real world, and to remove the harm of centralized finance, and build a truly decentralized financial world.

Utopia originally means "an imagined place" or "a perfect place", and it can also refer to the state of things in which everything is perfect. DarmaCash (DMCH) is a real financial world that is based on privacy and can create smart contracts to issue privacy stable coins. Through atomic exchange and Oracle, the value exchange between privacy stable coins and DMCH is realized, which allows a value exchange between a new financial world and the real world. We call this – DMCH Utopia.

3.1.3 Design Logic of DeFi/DEX

The following are the design logic of Dharma (DMCH) DeFi/DEX:

(1) Releasing Ethereum-based DMSwap. Please refer to 3.1.4 for more details.

(2) Issuing DSC (DarmaCash Stable Coins):

• Maker is a smart contract system on Ethereum that has provided the first decentralized and basic stable currency DAI (which can be simply understood as the US dollars on Ethereum) and a derivative financial system. DAI is issued through full mortgage guarantee of digital assets, with 1 DAI equaling 1 USD. Since its launch in 2017, DAI has always been linked with the US dollars, and DMCH will use the same protocol to issue the stable currency DSC of DMCH.

• The principle that DSC can become a stable currency is similar to that of DAI. DSC is always over-collateralized, which means that there are always sufficient assets behind DSC. If asset prices rise, then the DSC guarantee will be more adequate. If the asset drops to a certain value (the original CDP opener did not make a margin call or repay DSC), the contract will be automatically liquidated. Any user can liquidate assets that are under-collateralized, and get a 3% risk-free return. This will encourage many market participants to play the role of a keeper in Maker. They can not only benefit from the system, but also protect the solvency of DSC.

• Liquidity and redemption are important infrastructures for the success of DMCH. DMCH will distribute 20% of the overall emissions to LPs that provide liquidity for DMCH/DSC.

3.1.4 Ethereum-based DMSwap

In 2020, AMM DEX that is based on the concept of DeFi has witnessed an explosive growth. Ethereum has benefited from the popularity of the AMM Pool, with its ecology being further developed. In theory, the DMCH-based DeFi/DEX platform has a higher TPS and lower GAS than Ethereum, and it also supports privacy protection, which has greater potential than Ethereum. Considering that liquid mining has formed a siphon effect, and turned Ethereum into a dominant situation, DarmaCash (DMCH) will launch the DMSwap project that is based on Ethereum. The design concept of DMSwap comes from Uniswap and SushiSwap. Yet, unlike Uniswap, SushiSwap and other projects, DMSwap not only has various incentive mechanisms, such as user recommendation incentives, project recommendation incentives, transaction incentives, and token repurchase, but also received the anonymous blockchain Dharma (DMCH) as the value support in another dimension. DMSwap will eventually move back to the DEX system of DarmaCash (DMCH).

Based on the overall planning of the DarmaCash (DMCH) main chain project, we've designed the DMSwap project with the following main objectives:

(1) To verify the feasibility of a business model based on DMCH DEX and DeFi platforms;

(2) To provide a higher liquidity for DMCH by means of AMMPool;

(3) To grab and lock in market share before launching DMCH DEX and DeFi

platforms;

(4) To probe into the ETH ecosystem, and let the ETH ecosystem know more about DMCH.

Compared with Uniswap and SushiSwap, DMSwap has mainly innovated in the following aspects:

(1) Realized the user incentive plan (referral relationship), and considered GAS cost;

(2) Transaction dividends in a transaction have been created;

(3) The transaction gives the creator flexibility to define fees;

(4) A third-party address can be specified during the exchange process;

(5) Participants in the transaction can obtain DMS (DMS is the platform currency of DMSwap);

(6) 20% of the transaction fee is used to trade in DMS;

(7) The incentive plan of the project and a dual token incentive mechanism have been implemented, which means that if A does LP for B on DMSwap, A can not only get DMS, but also the incentive token of B project itself.

3.1.4.1 DMS

DMS is the token of the DMSwap protocol. Holding DMS means to have all the rights and interests of the DMSwap platform, as well as the right to vote for the development of DMSwap. All the DMS holders can vote for major decisions on DMSwap. At present, DMS can be obtained through four methods, that are – recommending DMSwap to other users, recommending DMSwap to other projects, becoming an LP for DMSwap, or making a transaction in DMSwap. Part of the trading fee will be used to trade in DMS.

3.1.4.2 DMCHE

DMCHE is an ERC20 token on the Ethereum blockchain, and supported by an equal amount of native DMCH (on the DarmaCash blockchain). One DMCHE is worth the same as one local DMCH, and users can transfer between DMCH and DMCHE at any time via DMCH-Bridge.

3.2 DarmaCash (DMCH) Instant Messaging Ecology

Instant messaging is part of the social network. As the most extensive infrastructure and open platform of the Internet, social networks have greatly improved the efficiency and speed of social interaction. Instant Messaging developed on the basis of DMCH network will be a next-generation social platform based on blockchain technology, and combined with DeFi, IM will be the first social financial application built on the blockchain. It will enable all DMCH users to have a sense of belonging, and socialize within a certain group.

3.3 DarmaCash (DMCH) Distributed Private Network Ecology

Distributed Private Network can be understood as a specific form of web3.0. The distributed private network based on DMCH, featuring anti-DDoS, anti-blocking, high speed and stability, has greater advantages than the current Internet infrastructure. DMCH's PPoS nodes rely on its economic incentive mechanism to form a globally distributed network (as shown below). When DMCH has enough PPoS nodes, a decentralized distributed small-world network is formed. This will make the shortest path between any two client-ends only 2-3 nodes away, and provide the most complete blockchain infrastructure for the decentralized application ecology of DMCH. On this basis, a distributed private network based on DMCH can operate all current Internet resources, including IP resources, domain name resources, content resources, etc. In this new small-world network, DMCH has redefined a brand-new Internet world for us.

Chapter 4 – Token Release Mechanism

4.1 Specifications

Total supply: About 460 million (467,440,737)
Consensus: PoW + PPoS
Algorithm: CryptoNight-R (CNR)
Block time: 15 seconds
Confirmation time: 90 seconds
Block size: 1.5 MB
Pre-mining: 3% (About 14 million), all donated to the DMCH community

4.2 Mining release

In the early stage, a part of DMCH was released through PoW mining. Since PPoS was released online, DMCH has adopted PoW+PPoS mining model, and most of the DMCH will be generated by PPoS mining.

4.3 Releasing Curve

DMCHv1 is the first stage, which adopts PoW consensus. At the beginning, every block releases 589 DMCH, which is halved once a month, and the mining lasts for 8 months.

DMCHv2 is the second stage, which adopts PoW + PPoS consensus. At the beginning, every block releases 7.4 DMCH, and 5% of which is distributed to the PoW miners, and 65% to PPoS nodes and users, and 30% is used as PPoS node operating rewards in the early stage, but the percentage is later reduced to 10%, as the remaining 20% is used as DMCH liquidity service reward. The block reward will be decreased block by block, and in the second year, the number of rewards is reduced by half, and after it is reduced to about 1%, it will be halved every four years, and the production reduction cycle will be determined as per community votes. DMCHv3 will adopt PPoS consensus.

4.4 Release Principle

The release and allocation mechanism of DMCH may be changed according to actual conditions. The principle of alteration is conducive to the further development of the project.

Chapter 5 – Roadmap

Time		**Plan**
2018	**Q1**	DMCH network R&D* Technological R&D of Block-DAG CryptoNote protocol optimization Ring signature optimization Bulletproof protocol optimization
2018	**Q2**	
2018	**Q3**	
2018	**Q4**	
2019	**Q1**	
2019	**Q2**	
2019	**Q3**	
2019	**Q4**	DMCH main net released online DMCH block explorer released online DMCH mobile wallet released
2020	**Q1**	Switch from PoW to PoW+PPoS
2020	**Q2**	DMCH EVM R&D Anonymous contract development Oracle optimization Technological R&D of atomic exchange
2020	**Q3**	
2020	**Q4**	VRF+PPoS R&D Anonymous token development Optimizing smart contracts Decentralized exchange DEX development
2021	**Q1**	VDF+VRF+PPoS R&D SDWAN R&D IM R&D
2021	**Q2**	
2021	**Q3**	
2021	**Q4**	

*R&D refers to “Research and Development”