HashFuture Whitepaper

CATALOG

We are in a fast-changing world of digital revolution.

Tech giants have, together and intentionally, monopolized our digital identities.

Say, Google has more than 90% market share in its search engine business. Facebook has 1 billion daily active users generating more read than that of the Bible. And Amazon earns 44 cents from every dollar of global digital marketing revenue.

Tech giant seats in the center of today's internet, controlling nearly all traffics and data generated by users. Feed by the data pipeline, they become a terrifying network of conglomerates squeezing every byte of profitable data from users with no respect on personal privacy. To them, users are no more than meats to be processed in a factory, or simply a money printing unit.

The damage caused by tech giants not only affects individuals but also impacts directly to small-and-medium sized enterprises (SMEs). For instance, Facebook was found to have leaked 87 million users' personal data, while Apple Inc. charge 30% "Apple Tax" on all revenue generated from mobile applications released on Apple Store. Individuals, SMEs and developers are no match for these giants.

Yet a new force is awakening at the middle of the Internet Dark Age, a decentralizing force which has the potential to overthrown tech giants' monopoly. In 2009, Satoshi Nakamoto established the first Bitcoin blockchain, arousing public interests on the potential of decentralized ledger. Then in 2015, Ethereum comes to life which advances blockchain technology to 2.0, embedding smart contract features. Since then, development of blockchain technology has accelerated to usages in different scenarios and expansion in processing capacity. These improvements signify the third generation of blockchain technology.

Blockchain technology prohibits unauthorized alteration on transaction history, increasing data security and at the same time reducing transaction costs. Better still, this technology allows everyone to take a role in decentralized ledger, inherently avoiding a single dominating player.

Given the enormous economic potential from blockchain technology, super powers like the United State, Russia and China have escalated blockchain development to a national strategy level. Application of blockchain is widening to most industries ranging from logistics to retailing, and from medication to marketing. Solely in 2017, global investment in blockchain projects had reached USD 2 billion and this figure is expected to grow three-fold in 2018.

That said, decentralized technology is destined to conflict with centralized technology.

According to Chris Dixon's point of view, the first stage of internet (1980s to 2005) laid a foundation based on open-ended communication protocol. The second stage (2005 to current), where tech giants like Google, Amazon and Facebook thrive, is based on booming mobile applications and development in Internet-of-things (IoT). And today, we are undoubtedly heading to the third stage of the Internet era, where blockchain technology highlights the possibility of a decentralized Internet.

This is an era with rapid advancement, replacement and achievement, attracting brilliant minds to participate in the digital revolution.

That's why we established HashFuture

HashFuture links the reality with the internet by educating the general public with blockchain-related knowledge using easy-to-understand live scenarios. In the digital world, data would be recorded in blockchain and all participating individuals can interact and trade equally without geographical constraints.

HashFuture is born to engage the value of equality, transparency and authenticity.

We firmly believe the shield of centralization will be penetrated eventually.

For Digitalization of modern society is a natural selection process and it is irreversible.

The upcoming internet would be one that embraces equal participation, fosters trusts, allows freedom of trade and supports mutually beneficial outcomes.

HashFuture commits itself to build a better internet using blockchain technology.

Our rewards are awaiting us at the end of this magnificent internet revolution.

What is HashFuture?

We are in the era of vast digitization and the current development of information technology encounters a prominent bottleneck on digital assets management. Ownership and transfer of digital assets are subjected to challenges on both initial recognition and subsequent transactions.

Current blockchain technology is not sophisticated enough to render an efficient solution on digital assets management since most blockchain projects are not designed to recognize multiple classes of digital assets. Even if a blockchain is compatible with digital assets, it is not tradable with mainstream blockchains, which restricts the value of the underlying assets. Enormous efforts and investments were made on ill-designed projects where failure is expected.

The mission of HashFuture is to advance on blockchain technology so to construct a solid foundation for digital assets management. HashFuture will overcome the roadblocks on ownership recognition and transaction recording of digit assets. To achieve this mission, a blockchain-based platform will be developed by HashFuture with distinct features on protocol layer, technical layer and application layer (All-encompassed design).

On protocol layer, HashFuture proposes the HashModel on ownership establishment and trade standards for digital assets after thorough considerations on different jurisdictions' legal requirements, social norms and market practices. On technical layer, a new technique, HashNode, will enable digital assets be traded between other blockchains in different scenarios. This would be a great step forward unleashing liquidity for digital assets. Then on application layer, HashWorld platform is available to the public in both website and mobile application. Its user interface is carefully designed with the greatest degree of simplicity, security and stability. HashWorld allows millions of users to begin their understanding on digital assets and get involved in assets management in the most convenient way.

Why HashFuture is needed in the Digital era

Pitfall in assets ownership recognition and transaction recording

Modern assets' ownership establishment like company incorporation and real estate transaction are heavily relied on physical documents. Document flow is lengthy and the parties involved have to communicate repeatedly to furnish all necessary documents. Worse still, individual's signature is exposed to unauthorized replication and a degree of subjectivity is embedded. Traditional assets are not free from document burden, not to mention intangible assets like algorithm, software, patents and copyrights. Due to the intangible nature of these intellectual properties, the problem of unauthorized replication is yet to be solved, resulting in enormous loss of revenue every year.

A new class of intangible asset has emerged which is different from tradition assets and intellectual properties mentioned above. It is phased as the gold of the digital era – Big Data. Big data originates from user's activities with different internet service providers, their e-footprints, point of view, social circle and even shopping preference are all recorded intentionally by service providers. Service providers then sold users' data in bundles to other commercial firms in return for profits. There is a much-needed breakthrough to protect personal internet privacy.

Transactions of traditional assets and intellectual properties are mostly recorded by industry service providers. Yet the outdated system used, lengthy procedures involved and aged equipment have created significant security risks in the aspect of ownership registration and transfer. Incidents of false contracts, loss of documents, fake signatures are not uncommon, pointing to a fact that a new decentralized solution is urgently needed.

Blockchain technology is the best solution to this problem. By adoption of blockchain on assets management, unauthorized deletion or alteration of assets ownership would be prevented. Efficiency on ownership transfer will be lifted drastically. Transaction procedures which require several months nowadays might well be shortened to minutes with blockchain technology.

HashFuture solution

HashFuture's solution is comprised of two core modules: (1) asset digitalization and importation module, and (2) cross-blockchain transaction module. Leveraging on blockchain fundamental infrastructures, HashFuture introduces improved encryption methodology and decentralized

consensus mechanism to sustain a complete, distributed and immutable ledger. This allows participants to conduct trade, store digital assets and retrieve information without the need to check counterparty's creditability (Trustless). Assets registration and transfer will be revolutionized under such scenario.
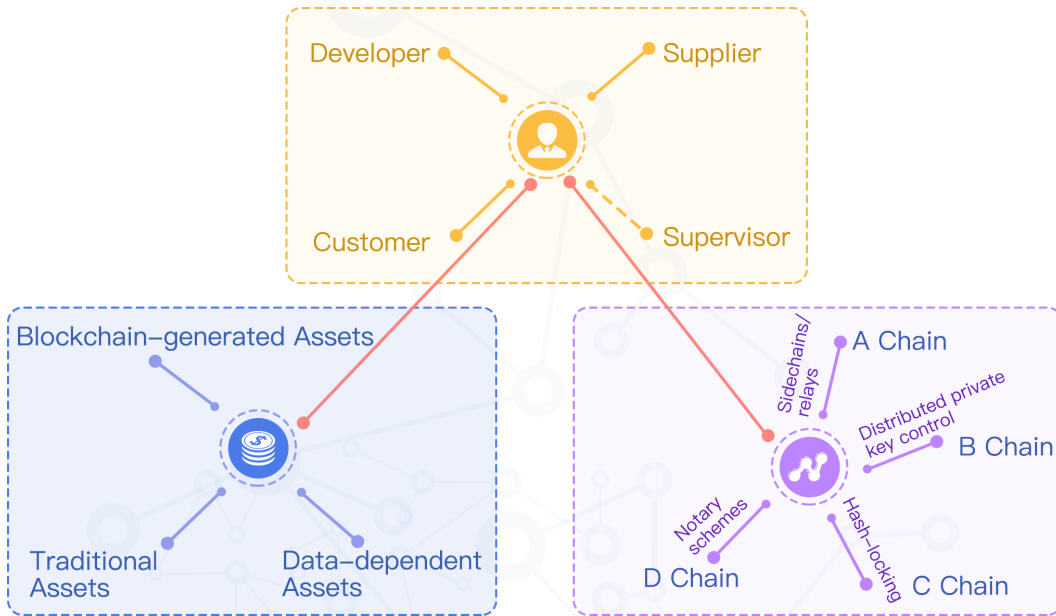

Figure 1: HashFuture Solution

Asset digitalization and importation module

HashFuture considers different jurisdictions' legal requirements, social norms and market practices to come up with the HashModel asset digitalization and importation protocol. HashModel standardizes how asset features are extracted, formatted and documented. It also introduces effective monitoring and user protection mechanism. The following three benefits can be achieved when assets are digitalized and imported to HashFuture's blockchain:

1) Increased asset information transparency and reduce counter-party risk

Prevalent assets management practices allow certain assets specifics to be hidden from due diligent check, resulting in transaction risk. Since a blockchain contains hundreds, or thousands of nodes which is visible for any visitors (each of which is a complete ledger of its own), manipulation of ledger on a single node would be detected by other nodes on the same network. The more nodes a blockchain is supported, the harder it is for hacker to outplay its computing power, thus deterring duplication of assets or any counterfeit products.

2) Increased settlement efficiency and reduce administration cost

Since decentralized ledgers are updated in real time with all exchanged data published in a global electronic publication platform, settlement of transactions is processed in real life with no undue delay. This helps boost the efficiency in digital assets transactions and also lowered risk of system failure because there is no dependency on a single ledger / node. Besides, ordinary procedures on ownership registration and transfer of assets require prolonged processing time and complex documentation. By adopting smart contact, transactions can be initiated and settled automatically, eliminating any unnecessary human resources and intervention.

3) Legal compliance and audit

Regulatory framework on blockchain projects or corporation is different, or simply do not exist, in different countries. HashFuture has continuous co-operation with legal counsels in major jurisdictions to ensure the whole project complies with International legal standards. Any local regulatory requirements on project / company registration will also be adhered.

Cross-blockchain transaction module

The system of cross-blockchain transaction is mainly comprised of four sub-modules, including ledger module, transaction integrity module, automatic translation module and interface module. Advancements are made based on existing protocols to reach consensus with other mainstream blockchain projects and communities (e.g. BTC, ETH, EOS). The cross-blockchain technology designed by HashFuture can shorten transaction lag time, improve privacy protection and achieve better security. Three distinctive advantages can also be achieved below:

1) Reduced credit risk

Blockchain is inherent to have the character of open-sourced and transparent. Participants are aware of execution rules defined and they can manually verify the completeness and authenticity of transaction history. With ledger trackability and automatic execution of smart contract, users' credit risk exposure is minimized.

2) Prevent double spending

Existing blockchain projects are mostly isolated and not compatible with each other. It is possible that asset owner might abuse on this situation and import digital asset simultaneously on multiple discrete blockchains. With HashFuture's cross-blockchain solution, asset status will be communicated across all partnership / compatible blockchains, thereby preventing the loophole of double spending.

3) Improved assets liquidity

Isolated blockchains are confined with a small number of user base and a finite scale of assets. Trading volume and asset liquidity are greatly restricted given these dilemmas. Once assets can be exchanged across different blockchains, trading volume shall be boosted instantly, attracting more market participants and injecting a vast amount of liquidity to the market.

Mission and values of HashFuture

To formulate a liquid, secured, creditable and community-governed digital assets eco-system has always been HashFuture's' primary mission. If achieved, HashFuture will become the next Alibaba in the era of digital assets.

HashFuture team upholds the following values ever since its establishment:

1. To empower individuals with ownership and liquidity on their digital assets by connecting reality with the internet and constructing linkages between individual blockchains.

2. To forester healthy development of the blockchain community by stressing the importance of technical advancement. Innovations shall be set free and then be examined prudently upon application.

3. To encourage acts that benefit all contributors of the community.

Blue map of HashFuture

Once the technical difficulties on ownership establishment, transaction efficiency and assets security be resolved, HashFuture will become the most significant trading platform of all blockchain-generated assets, digital assets and traditional assets. HashFuture will also release its organic blockchain technology to external parties to accelerate overall development of blockchain community. HashFuture provides infrastructure on protocol layer, technical layer and application layer, forming a strong bonding with the HashFuture community. This self-sustaining eco-system would be able to refine and refresh itself.
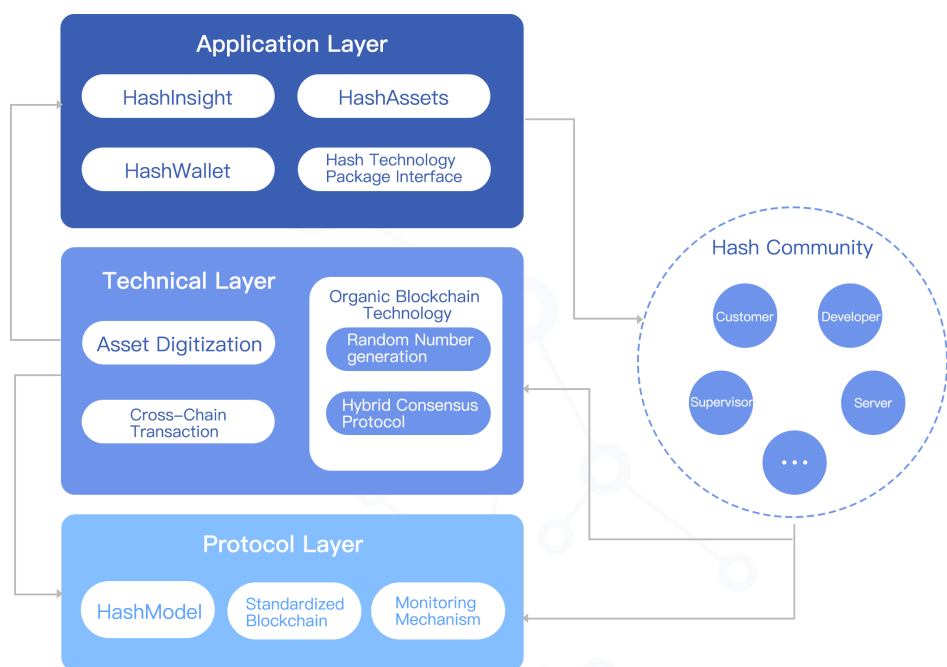
Figure 2: Blue Map of HashFuture

Protocol layer

Introduction:

There are different classes of traditional assets in real life. Ownership recognition and transaction recording of these assets involve problems in jurisdictions, languages, legal system, commercial norms and the like. Same set of problems must be addressed when traditional physical assets have a corresponding identity created in blockchain. HashFuture will construct a blockchain-based common standard protocol to encompass assets diversity and the complexity associated.

Similar to TCP/IP standard solving the problem of data transition between servers and unlocked the golden era of Internet, the HashModel advocates by HashFuture allow assets be traded both offline and online, penetrating the boundary between real world and the Internet.

In terms of assets classification, currently assets can be divided into three classes: Blockchain-generated assets, data-dependent assets and traditional assets. Example of blockchain-generated assets include Ethereum token and Ethereum Kitties. Creation, utilization and transaction of blockchain-generated assets are closely related to the underlying blockchain. Ownership of blockchain-generated assets is hosted in a digital wallet address, transaction is processed via smart contract and user rights are defined according to mechanism designed by the founding developers.

Different from blockchain-generated assets, the scope of data-dependent assets is much wider for all digital information expresses in "byte" belong to this class. However, data-dependent assets have a high degree of ambiguity when it comes to ownership issue and thus are easily subject to abuse by database owners. This is because data-dependent assets are mostly originated from users' interaction with various platforms and service providers. Texts, photos, videos uploaded by users are easily understood as data-dependent assets. Indirect information such as users' browsing history and behaviors are also within this assets class, adding complexity in identification of assets ownership.

And since data can be replicated inherently, traditional business model fails to profit continuously from sales of data, demotivating people to refine and extract useful information. Consequently, we can observe that platforms and service providers are earning their cash flow not from sales of data but from sales of traffics and publication of advertisements. With HashModel, ownership and transaction issue of data-dependent assets will be resolved, releasing the full potential of big data.

Traditional assets include tangible assets like real estate and vehicles, and intangible assets like patents and trademarks. This asset class will not be free from reformation in front of the digital era. With the continuously development of financial market, equity securities and derivatives are fully digitalized and therefore become compatible to blockchain technology. Decentralized trading of equity securities and derivatives become possible with greatly settlement efficiency and security on ownership.

HashModel is a blockchain-based common standard protocol designed by HashFuture team. It defines how different asset classes are 'imported' into blockchain and be exchanged across blockchains. HashModel utilizes the concept of class structure in computer science and leverages on relational chain to accommodate as many asset classes as possible. This brings the HashModel more flexibility and wider asset coverage.

Any individual on HashFuture platform can develop ownership recognition and trading mechanism of a specific asset class based on the HashModel. If such mechanism is widely accepted and adopted in the HashFuture community, then the HashFuture Foundation will reward Hash tokens to the developer via smart contract according to benchmarks such as number of users, trade volume and trade values etc. When more and more asset classes are made available in HashFuture, Hash token as the only means of exchange will gain increased valuation support.

Implementation:

Protocol layer allows linkage to be constructed between reality and blockchain. This very first step will extend to a full solution of assets digitalization which can be apply to both tangible and intangible assets. The following diagram illustrates the function of sub-protocols.
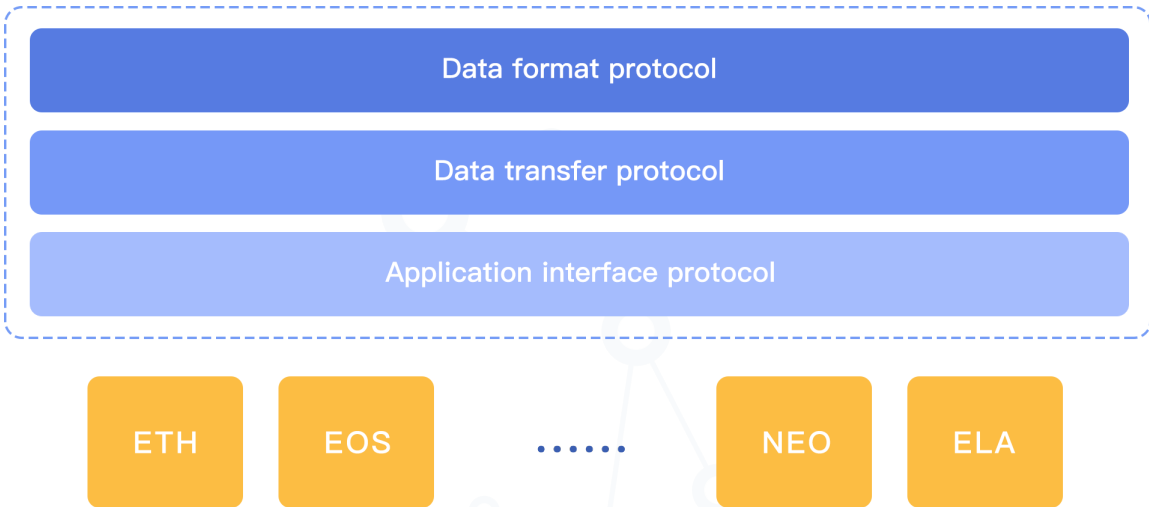
Figure 3: Sub-protocol Logic

1. Standardized blockchain relationship: Protocol layer is defined above and across different discrete blockchains. Such protocol is named as Open Blockchain Architecture Interconnect Protocol (OBAIP) which is a common standard for blockchain data storage and exchange. As shown in figure 3, even though different blockchains have different structure, data format and data transfer protocol are independent from blockchain structure. The function of OBAIP is to eliminate roadblocks arising from differences in various blockchain structures. OBAIP is a combination of:

   a. Data format protocol: Rules governing data format, coding and encryption

   b. Data transfer protocol: Rules governing inter-blockchain data transmission

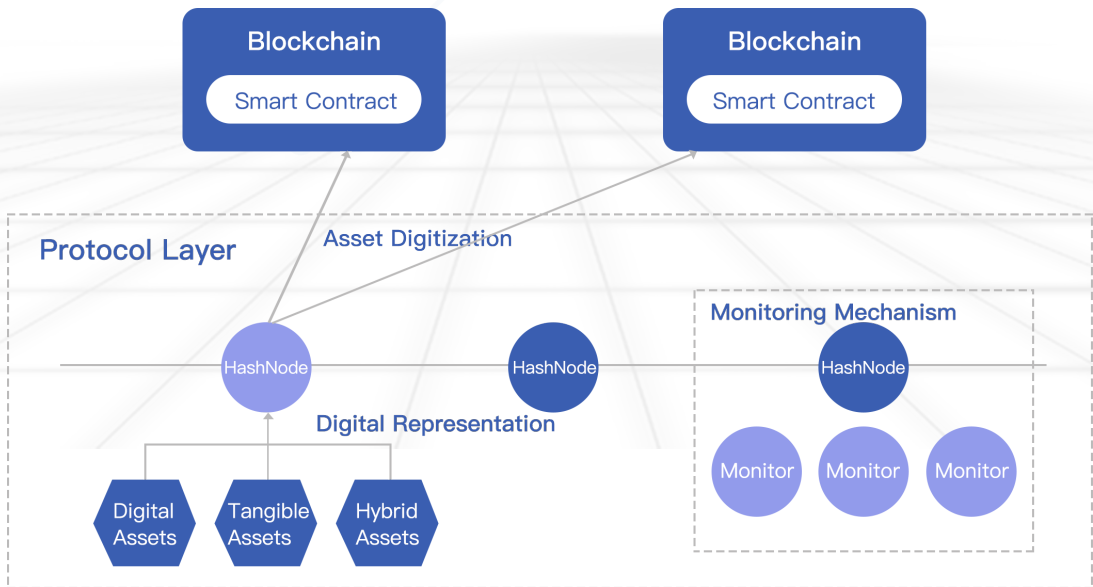   c. Application interface protocol: Interface between HashFuture and user-oriented applications

Figure 4: Function of the Protocol Layer

2. Formulate standardized digital asset features (HashModel): to capture key features of the three asset classes discussed previously, we focus on the following key characters:

   a. Data format protocol: Rules governing data format, coding and encryption

   b. Data transfer protocol: Rules governing inter-blockchain data transmission

   c. Application interface protocol: Interface between HashFuture and user-oriented applications

   HashFuture provides Domain Specific Language (DSL), a simply and general programming language to help protocol developers visualizing their codes.

3. Formulate standardized blockchain features: In this aspect HashFuture concerns how the same piece of asset is presented in different blockchain structures (Say ETH, EOS network). One example is ERC721 contract used in the Ethereum blockchain, it can be used to represent certain unique asset. However, ERC721 contract itself is not compatible with Bitcoin's blockchain structure and thus cannot be recorded. And it is nearly impossible for Bitcoin's fundamental blockchain structure be amended to accommodate ERC721 format. Having that said, HashFuture's strategy is to extract common fields among existing blockchains to ensure OBAIP covers as many mainstream blockchains as feasible. Ultimately, HashFuture aims to promote OBAIP format as the industry standard format for upcoming blockchains.

4. Design an effective monitoring mechanism: Generally speaking, no matter how a protocol is well designed, there is still risk that assets might be duplicated, whether due to error or fraud. To resolve this issue, HashFuture places a HashNode on each asset import portal (Shown in figure 4). HashNode has the following functions:

   a. Temporary storage of assets

   b. Extraction of asset features

   c. Actual import of asset to blockchain

Monitoring mechanism is meant to add transparency to the three steps mentioned above. With transparency, a subject asset can be verified on its existence, ownership and uniqueness. To introduce transparency, HashFuture would allow participants to act as verification agent. If we view various blockchain projects as verification agents (HashNode), then actual monitoring would take place across blockchains instead of within HashFuture's blockchain. Therefore, a streamlined assessment workflow (e.g. voting, random selection) can be designed to engage external parties as verification agents. Hash Token will be rewarded to all participants who assist in this process. Assurance of asset authenticity is achieved here.

Technical layer

Introduction:

Blockchain technology is undoubtedly the most effective and efficient tool for digital assets recognition and transaction at horizon. For assets to be imported to blockchain and then transfer across different blockchains, a consistent technical solution must be in place which is compatible with other blockchain projects.

For assets digitalization and recognition, on Protocol layer HashFuture has already designed Data format protocol to covers structural inconsistency among different blockchains (e.g. EOS, ETH, BTC). At Technical layer, HashFuture has well-designed algorithm to execute calculations efficiently.

Whereas for inter-blockchain asset transactions, critical factor for asset liquidity, we define the following parameters for illustration purpose:

Definition 1: For any blockchain network A, B (Where A, B are equivalent to nodes in their corresponding blockchain network)

a. A and B can process any legitimate orders (announcement of result, verification of transaction, package data into blocks etc.)

b. A can obtain all information stored in B via certain communication protocol. The reverse from B to A is also true.

c. A can act correspondingly to information stored in both B and itself. Same for B.

A subset of definition 1, for example, is inter-blockchain transfer between BTC and LTC. Say Alice and Bob need to conduct a transaction which converts BTC to LTC, 2 steps are involved in this scenario. In BTC network, Alice transfer certain amount of BTC to Bob; whereas in LTC network, Bob transfer an equivalent amount of LTC to Alice. Needless to say, overall BTC value and LTC value of each blockchain remain unchanged immediately after completion of such transaction.

Besides from exchange of cryptocurrency, HashFuture is trying to address a more fundamental problem of assets circulation. Say there is a physical sportswear being digitalized and imported to blockchain network A, and then the digitalized image of this sportswear is transferred to blockchain network B. Naturally, the primary digital image of this sportswear in blockchain network A must be reduced. We have a second definition here for illustration:

Definition 2 (HashFuture assets transfer):

For any blockchain network A, B:

VA= { x | x ∈ A } means sum of value in network A,

VB= { x | x ∈ B } means sum of value in network B,

x ∈ A means x is recorded in blockchain network A via any legitimate order

A transfer of asset from blockchain A to blockchain B, for x ∈ A, the status of blockchain A immediately after the transfer should be:

$$V'A = VA \setminus x$$

$$V'B = VB \cup x$$

As blockchain is a class of open ledger, each blockchain project represents a discrete ledger and there is no linkage between different ledgers. If we shift our viewpoint from blockchain to individual user, if she can transfer a certain asset stored in one ledger to another, then such asset would become more liquid and more valuable. Technically speaking, two principles must be obeyed to achieve inter-blockchain transaction:

1. Integrity of transaction. i.e. Reduction in network A must match with addition in network B.

2. Traceability. i.e. Asset features recorded in network A, after transfer to network B, must keep the original asset features (e.g. Sportswear recorded in blockchain A is still recorded as a sportswear in blockchain B after transfer).

To satisfy the 2 principles discussed above, HashFuture provides a set of reliable and decentralized solution to support inter-blockchain transactions. Beside technical advancement, HashFuture has partnered with other mainstream blockchain projects and their respective communities. These strategic partnerships render supports in improving speed of transaction recording, assets security, data privacy, assets digitalization and inter-blockchain conversion etc. Simultaneously, HashFuture is actively looking for actual real live scenario for application of its blockchain technology. With a real live application example, the trust feature of blockchain can be observed and released.

Implementation:

1. Assets digitalization and importing is breakdown in two sub-processes:

   a. **Extraction of assets features**

   b. **Importation of asset features to blockchain network**

With respect to a, different asset classes require tailored-made process to summarize its asset features. In the case of blockchain-generated assets and data-dependent assets, this process is relatively easier because

both asset classes are already in digital form. While for traditional assets, the situation would be more complex as blockchain technology standalone cannot resolve the problem of double spending (or asset duplication). Asset duplication is possible when digitalization of physical asset take place, asset owner may retain a softcopy of asset features imported to blockchain network, and then claim the backup softcopy as original.

To close this loophole in traditional assets, HashFuture introduce monitoring mechanism to streamline the digitalization process. As shown in figure 4, the monitoring mechanism itself is an alliance chain which can be manually intervened if necessary. Any user who want to extract asset features of a traditional asset must strictly comply with the requirements in Protocol layer. To claim ownership over a traditional asset, user needs to reach agreement offline and then upload the agreement online to the alliance chain to keep record of data source. Records in the alliance chain will be published amount HashFuture community and therefore subject to public scrutiny. Meanwhile, HashFuture is also conducting development on supply chain technology (mainly hardware) to assist extraction of asset features in physical assets.

For b, the following factors are key concerns:

1. Capacity balancing: According to the dynamic capacity status of different blockchain networks, select the best assets digitalization portal.

2. Automation: Smart contract is designed corresponding to all blockchain networks which fit with HashFuture Protocol layer requirements. HashNode is positioned to be an easy-to-use API interface for external parties to develop related applications.

3. Exclusiveness: Asset owner has 100% ownership over the digitalized asset after importation to HashFuture blockchain.
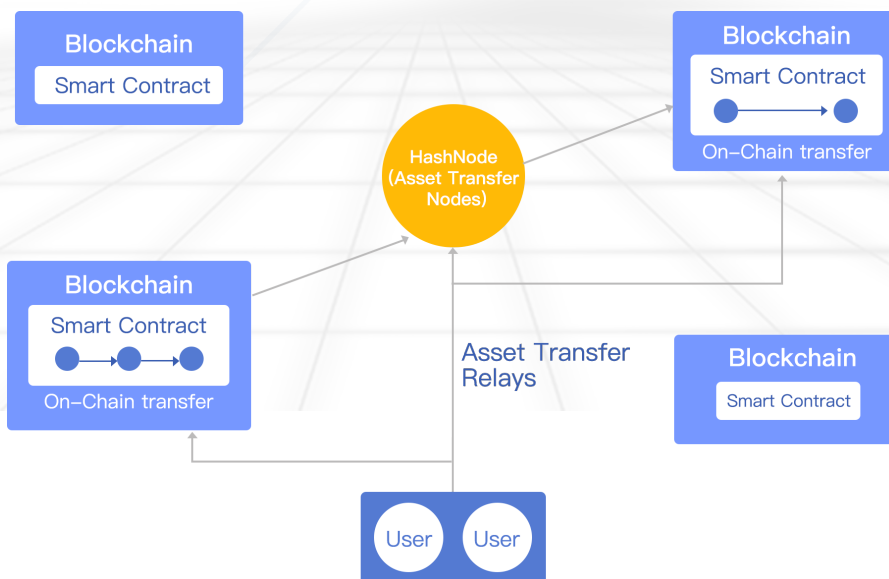

Figure 5: Inter-blockchain Asset Transfer Diagram

2. HashFuture aims at providing an all-rounded and sophisticated solution for inter-blockchain asset transactions. Currently there are 4 mainstream inter-blockchain transaction technologies in the market, they are: Notary schemes, Sidechains/relays, Distributed private key control and Hash-locking. These techniques are mainly applied in the following scenarios.

   a. Asset transfer to and from different blockchain networks

   b. Simultaneous exchange of assets between blockchains

   c. Cross-blockchain data verification

   d. Cross-blockchain execution of smart contract (e.g. securities recorded in blockchain A to pay dividend in blockchain B)

   e. Blockchain exchange (to supplement blockchain projects which are not supported in HashFuture Protocol layer)

The solution proposed by HashFuture is taking merits of all the existing technologies listed above.

Two technical problems have to be addressed here:

1. Inter-blockchain asset transfer

2. Decentralization

Technically, these are two distinct objectives (like ledger structure, centralization resolve the problem of transfer, while decentralization resolve trust problem) and therefore HashFuture would introduce a two-in-one solution.

First, a multi-centered Hash-Intermediate-Node (A special form of HashNode) is constructed, focusing on the problem of inter-blockchain asset transfer (Focus on fulfillment of Protocol layer requirements). As shown in figure 5, our solution is named as Centralized Hybrid Cross-chain Solution (CHCS) which is comprised of several modules.

   a. Ledger module: detailed transaction recorded to provide trackability.

   b. Transaction integrity module: Adopt improved Hash-lock and digital signature (or more powerful smart contract) to safeguard transaction integrity.

   c. Automatic translation module: compatible with different blockchain networks and perform auto-translation of assets feature format.

   d. Interface module: User-facing API, focusing on simplicity.

API adopting CHCS can accomplish inter-blockchain asset transfer and asset ownership can be located. In second phase, decentralization of Hash-Intermediate-Node will be conducted. For efficiency and security concerns, Hash-Intermediate-Node will be a public relay chain. CHCS will also be upgraded to Decentralized Hybrid Cross-chain Solution (DHCS).

HashFuture will form strategic partnership with other mainstream blockchain communities to provide support on inter-blockchain transaction technologies, increasing transaction recording and settlement speed, data privacy and data security. Ultimately, digitalization of different asset classes can be materialized and transaction among different blockchain networks is made possible.

Set aside the problem of processing efficiency, operation of inter-blockchain transaction requires the following two criteria be satisfied:

a. Consistency: Ledger recorded in full nodes must agree with each other (only allow transactions before network confirmation be different).

b. Liveness: Transaction arising from user-end will ultimately be written into ledger of full nodes.

In CHCS system, since it is a centralized mechanism, it can satisfy requirement a and b stated above with high efficiency (Assuming good standing of master node's integrity). When CHCS is upgraded to DHCS system, then new algorithm must be designed to accommodate the three requirements above. This algorithm is named as Consensus algorithm with key parameters defined below:

$$\min \quad \lambda_1 q + \lambda_2 dt$$

Where:

q means system capacity TPS (Transaction per second)

dt means average time needed for one transaction to be recorded

λ_1, λ_2 are weighting factors between efficiency and capacity

Although recent development of DAG allows POW to improve capacity q, the problem of prolonged recording time (dt) would exist permanently. Given the same computing power, recording time (dt) is a factor of actual time lapsed under POW mechanism. Not to mention POS and its derivative DPOS are both not decentralized.
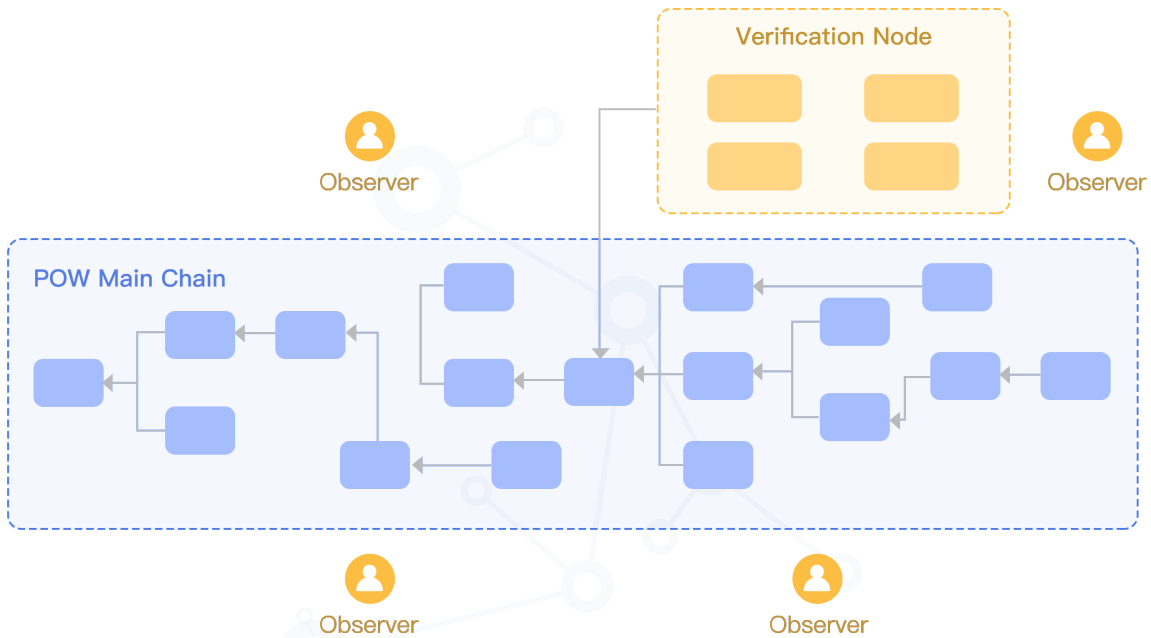
Figure 6: DHCS Public Chain Diagram

HashFuture uses hybrid consensus protocol. Its master chain adopts traditional POW mechanism. To increase processing capacity of master chain, directed acyclic graph method (DAG) is introduced. With the combined advantage of POW and DAG technology, processing capacity (q) of HashFuture master chain can significantly outweigh BTC blockchain network.

To reduce recording time (dt), HashFuture references to DPOS technique and suggests formation of witness node (Also known as verification node). Witness nodes are responsible for data record ordering in the master chain. To ensure smooth operation of the entire HashFuture network, Observers are introduced to capture abnormalities between master chain and witness nodes. These abnormalities violate the principles of consistency and liveness, an example would be a transaction initialized from user end is not confirmed nor recorded in master chain after a prolonged period of time, or such request is confirmed but not recorded in master chain. The hybrid consensus mechanism discussed above can significantly improve processing capacity of the master chain (q) and shorten recording time (dt) while maintaining the core value of decentralization.

Application layer

Introduction:

HashFuture targets to provide easy-to-use asset digitalization and transfer tool for the general public who might not have an in-depth understanding of blockchain network. Built-in Protocol layer and Technical layer algorithm will be made available to developers as API, so they will be able to share a slice of benefits in the upcoming HashFuture eco-system.

Implementation:

As of today, HashWorld application published by HashFuture already has more than a million active users from over 50 countries. HashWorld is a strong linkage between real world and the blockchain network providing usage scenarios and allow general public to experience how a blockchain network is look like. Hash Token (HSC) is the common currency circulating among HashWorld products and can be converted into other form of digital assets like virtual lands and buildings. Participant of HashFuture community who holds HSC will be able to enjoy HSC appreciation when HashFuture develops into blockchain industry leader. With sophisticated blockchain technology, HashFuture will be able to challenge tech giants 'monopoly and reward all earlier supporters with wealth in the digital era.

HashWorld eco-system

Individual who are not familiar with blockchain knowledge or blockchain-based projects could build their initial understanding within HashWorld mobile application by way of playing mini games. There are three core modules to complete the eco-system: HashInsight, HashAssets and HashWallet.

HashInsight: New token gateway

HashInsight adopts artificial intelligence in content selection algorithm to recommend user-specific blockchain related contents for individual reader.

These contents could be in the form of newsfeed, mini games invitation or daily mission. When users complete designated target, they will be rewarded with certain number of tokens. This is to boost user loyalty on a regular basis and thus maintain overall stickiness of the HashWorld platform.

HashInsight's artificial intelligence would collect user's behavior data and conduct segmentation continuously to distinguish their area of interests and knowledge level on blockchain technology. By so doing, HashInsight AI is the optimal learning center for the public to experience blockchain application.

Precise advertisement delivery can also be achieved to satisfy corporates marketing needs. HashInsight AI can dynamically match potential customer features as specified by corporations with individual user's interest portfolio. Businesses can reach out to their real target audience and user can read contents that they truly value.

HashAssets: ERC721 Type trading platform

Assets digitalization is one of the greatest usages of blockchain technology. Currently in HashWorld application, virtual land and buildings are being traded and bid to educate users on the value of digital

assets. Going forward, HashFuture will empower different industries with its Protocol layer and Technical layer technology to digitalize various asset classes, providing decentralized trading services and cross-blockchain asset exchange services. It will be the very first TaoBao supermall for digital assets being traded on decentralized and trustless environment.

The scope of digital assets applicable ranges from intangible items such as virtual gaming items to intellectual properties, and from digitalized tangible items like antiques to luxurious consumables. Different trading methods are also available including declining pricing model, bidding model and Peer-to-peer model. A holistic asset trading solution is provided to accommodate different commercial needs.

HashWallet: Scenario-based token wallet

Ownership of HashWorld token is the simplest and most direct form of participation in HashFuture community. HashWallet provides token storage and management services to end users via mobile application. Depending on users' feedbacks and needs, value-adding functions such as token exchange, token fund management and token payment might be incorporated into HashWallet. As compared to other token wallets on the market, HashWallet has an edge on user loyalty and platform stickiness thanks to HashInsight and HashAssets.

Infrastructures provided by HashFuture

HashFuture renders the following infrastructure to all dedicated developers and community members.
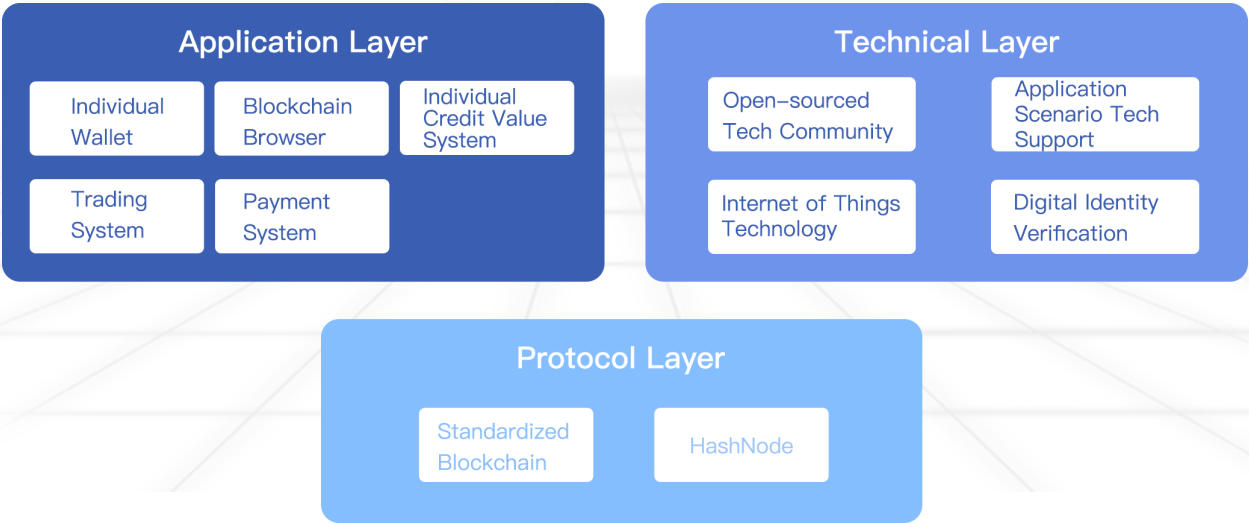

Figure 7: HashFuture Infrastructure Illustration

Protocol layer facilities

Trading is the one of the most long-existing behavior of mankind and is also one of the most legally regulated areas. Since barter trading in ancient time, then advance to oral promises and written contracts, trading terms and legal norms are building blocks of modern civilizations. There are two core problems surrounding development of trade-related legal framework: recognition of assets ownership and transfer of such ownership. In terms of assets ownership recognition, traditional solution is by government guarantee. This is true in modern world where movable assets, immovable assets and intellectual properties all need to be acknowledged and documented in government database.

Naturally, ownership recognition is the corner stone for subsequent trade and transactions. In the perspective of blockchain transaction, assets digitalization is an innovative form of ownership recognition and could allow transaction be completed in a ground-breaking manner.

HashFuture develops the revolutionary HashModel protocol framework to resolve the problem of assets digitalization and cross-blockchain assets exchange, addressing the questions of offline-online ownership consistency, offline transaction protection and online transaction disputes.

1) Offline-online ownership consistency

According to different asset class, HashFuture would first verify and cross check asset ownership via third party confirmation like notarization and witness by attorney. This is a crucial step to establish a trackable record before assets are being digitalized and imported to blockchain and warrant the underlying assets with a higher confidence level among public.

Different ownership recognition methods would induce different trading methods. Physical delivery of goods (e.g. vehicles / real estate) and actual transfer of certificates / vouchers (e.g. share certificate / bonds) are traditional settlement methods. Transaction cost of traditional trade settlement is high because a centralized governmental body is always needed to warrant legitimacy on the transaction. As such, buyer and seller must prepare documentations and pay any form of tax required by the centralized body. Numerous example can be found including filing of real estate transaction in land registry, stamp duties on bought and sold note of company shares and transfer of bond subscription agreement etc. In a blockchain based ownership recognition system, as far as asset ownership is confirmed on the very first instance during digitalization and importing, then such ownership need not be verified again in all subsequent transactions. The principle of offline-online ownership consistency and the mechanism put in place to check asset ownership upfront can significantly, or even completely, reduce trading transaction cost.

To satisfy global trading standard, HashFuture would adhere to the Common Law system which is used in HKSAR, the United State and Britain. This is because Common Law system is more widely accepted worldwide then other legal system like the Islamic legal system which is prevalent in Middle East only. Besides, court cases and court determinations under Common Law system are more generally adopted in other scenarios.

With the implementation of offline-online ownership consistency checking mechanism, standard trade flow and standard smart contracts can be designed to cater for mainstream asset classes. Asset will be highly liquid after blockchain standard contracts are put in place.

2) Offline transaction protection

Blockchain trading platform must be supplemented by a well-designed legal framework. The legal framework not only provides assurance on ownership recognition and transaction settlement, but also form an important part on risk management of the underlying assets. Legal framework applicable on traditional transactions is very well documented and organized given a long history of execution. Whereas for blockchain-based transaction, legal framework is nearly empty as this is an unseen form of trade. Given the lack of monitoring and tracking mechanism, HashFuture would put in place the very first set of blockchain transaction regulation, holding contract breaching party responsible for her improper acts and erasing all benefits so obtained in unjust transactions. This is a very meaningful step forward to protect trading parties and investors.

To begin with, asset ownership recognition will be conducted according to legal requirements applicable to different asset classes. Verification will be mainly completed by notarization, witness of attorney, entrust to insurance agency or confirmation by a professional blockchain trading agency.

If asset ownership is complex and asset nature is risky. HashFuture will formulate clear assessment procedures and demand written confirmation from valuation firms / institution who issue notarization certificate. All ownership certificates and vouchers will also be uploaded to blockchain to provide documentary support.

Further, substance of trade is about exchange of rights and obligations on the underlying assets, this has to be done via physical delivery, actual transfer of certificates or registration in governmental bodies. As a mirror image, HashFuture will establish a designated blockchain trading service institution which can hold assets on behalf of clients, accept pledge of assets and receiving deposit etc.

Through the above-mentioned arrangements, HashFuture will gradually disclose its blockchain algorithm. These open-sourced algorithms will collectively become standard regulations governing all

assets and transactions which is named as the HashModel. With HashModel, assets digitalization, ownership recognition, transaction recording and offline-online ownership consistency can all be executed and maintained. Inter-blockchain asset exchange is made possible, creating unseen liquidity for digital assets and providing a safe and convenient way for owners to trade.

3) Handling online transaction disputes

To resolve disputes happening on blockchain transaction, HashFuture would reference to existing regulation and social norms generally accepted by the public. HashFuture community members are also encouraged to suggest regulation standards. Once user promote themselves to be one of the HashNodes in the HashFuture blockchain, she can take part in accepting entrusted assets, importing digitalized assets, and proposing solution to disputes etc.

Individual service provider who join the HashFuture community can conveniently reference to open-sourced HashModel protocol to reduce time and cost on initial exploration. For developer working on Protocol layer add-ins, coding can be based on published HashModel, then application for specific scenarios can be created more efficiently. As new-born HashModel add-ins are distributed and quoted, developers are rewarded with corresponding number of tokens.
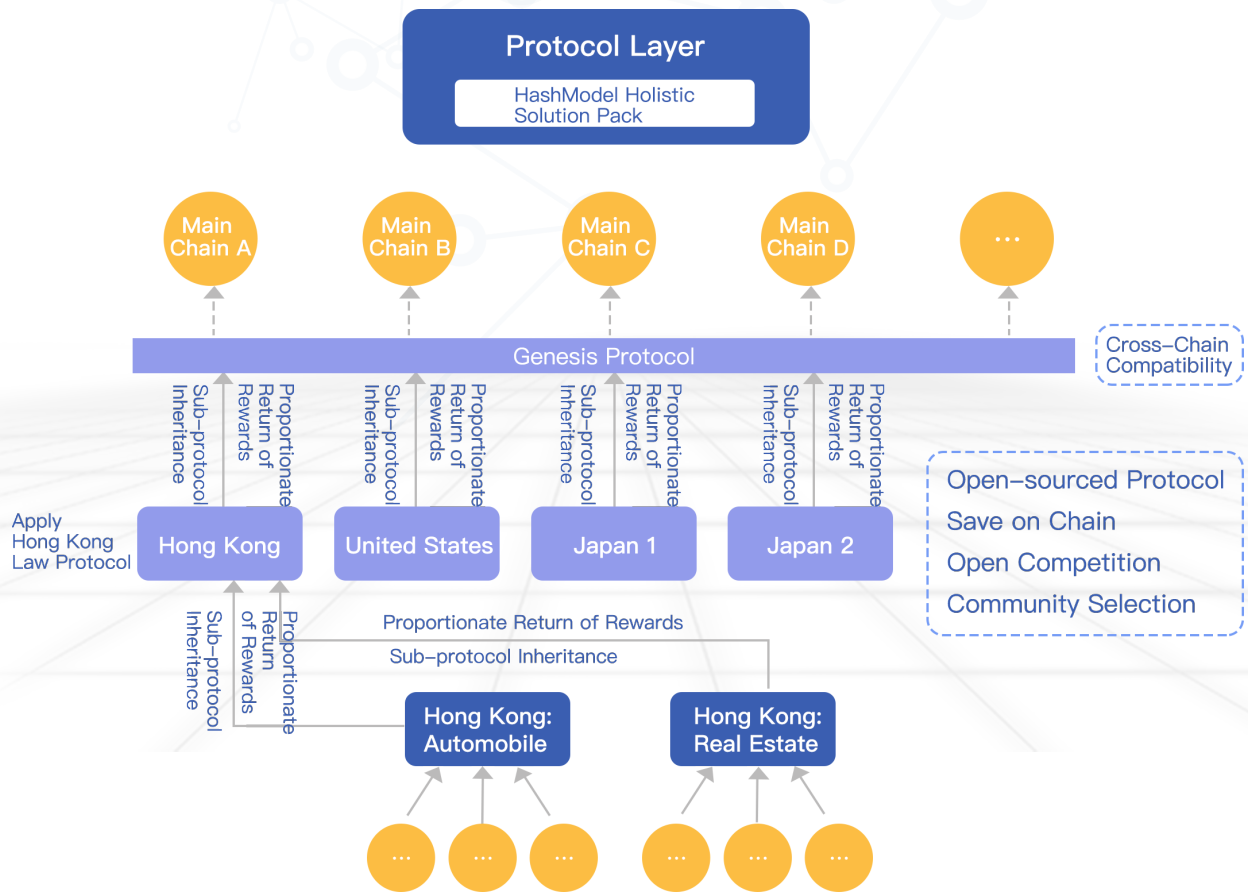

Figure 8: HashModel Structure

To sum up, solutions are provided by HashFuture on Protocol layer to handle asset ownership verification, ensure offline-online ownership consistency, offer offline transaction protection, resolve online transaction disputes, allow cross-blockchain transactions and provide flexibility on different pricing models. This holistic solution pack is the core foundation for regulations among blockchain industry.
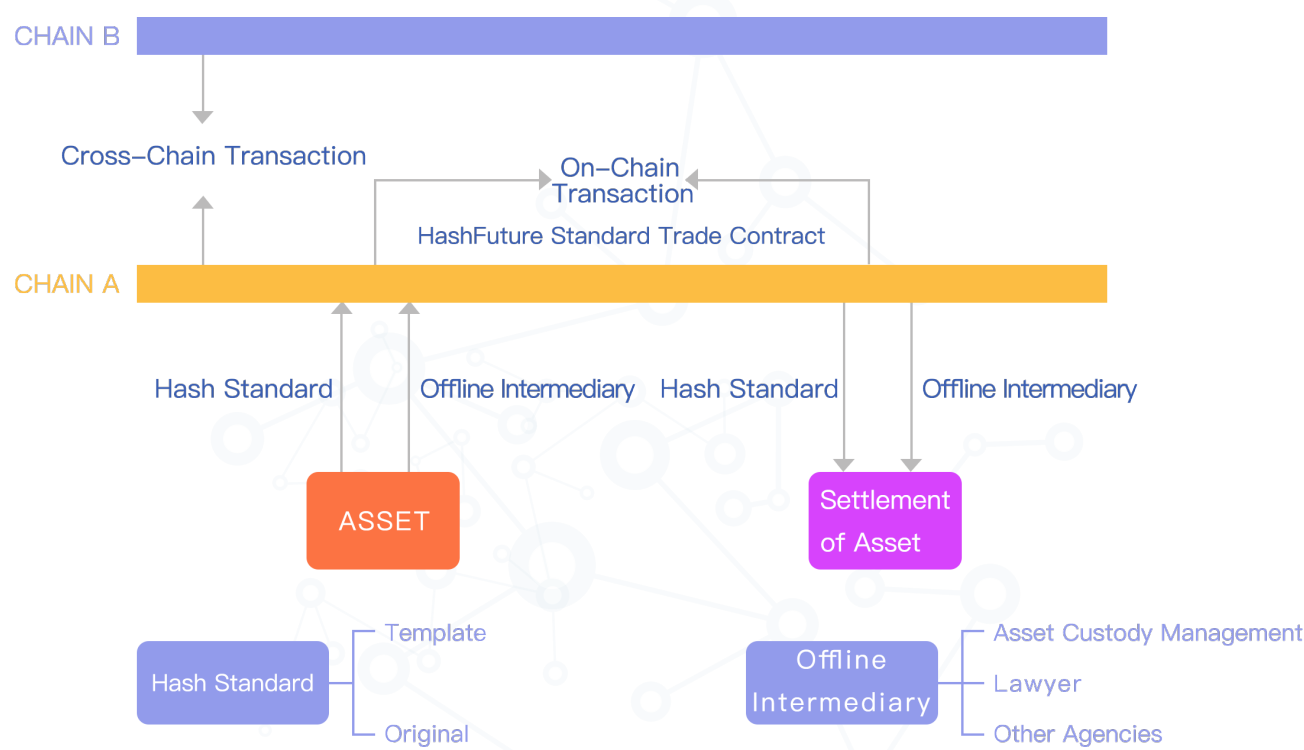

Figure 9: HashFuture Trading System

Technical layer facilities

Technical layer facilities are inherently compatible with HashFuture's Protocol layer standards and are positioned to provide technical support for application layer facilities. HashFuture will also make technical layer facilities available for other external blockchain projects.

1) Open-sourced community

HashFuture is committed to facilitate advancement of blockchain technology, inclusive but not limited to consensus mechanism, P2P network, distributed data storage technique and data encryption methodology. HashFuture pursues theoretically-sound blockchain infrastructure which is rigorously examined having real life usage. All resources developed will be shared with the HashFuture community as goodwill.

2) Scenario-based solutions

Blockchain-related theory and academic research must be down to earth with real life application. HashFuture would release decentralized technology together with cross-blockchain solution for external parties and community members to further create scenario-based applications. E.g. Auto-generation of verifiable random numbers.

3) IoT technology

To achieve the highest degree of accuracy and reliability on asset features verification and importing, HashFuture will develop IoT devices which are compatible with Protocol layer and Technical layer algorithm. These IoT hardware will collect information such as location, photos and other sensor-generated signals of the underlying assets. Valuation of asset depends on the overall feedbacks from these IoT devices.

4) Digital identity verification

Unique digital identity verification technique is available to ensure asset ownership recognition and importing is accurate.

Application layer facilities

1) Individual credit portfolio system

Benefiting from decentralized Hyperledger system design, any individual in HashFuture would have her own digital identity. Real life identity and the corresponding digital identity each would have its own credit history and portfolio. Accordingly, when identity set perform different actions or make decisions online or offline, new data can be feedback to blockchain system to write into the credit portfolio. This allows 360-degree examination and recording of user's identity set, which can permanently eliminate the prevalent dilemma of BOT-generated traffic. With the individual credit portfolio system, users' creditability can be fairly reflected within HashFuture and applications can entrust the credit portfolio for analysis or to provide service.

2) Exchange

HashCoin-oriented exchange is offered for users to trade HSC with other cryptocurrencies or traditional sovereignty currencies. No levy nor administration fee is charged on transactions and all trade records are transparent on open ledger.

3) Payment and clearing system

Payment system ensure HashFuture community members are protected when they consume HSC, other cryptocurrencies or traditional sovereignty currencies to purchase goods and services online. Only when both buyer and seller confirm a transaction will the payment system transfer considerations from buyer to seller. Again, all transaction records are made available on the open ledger to provide transparency.

4) Digital wallet

Each user has her own digital wallet to record token balance and its corresponding value. The wallet can also hold token on behalf of other users. Payment and receipt history is recorded automatically. HashFuture aims to render simple and reliable digital wallet API for all users.

5) Blockchain browser

Blockchain browser is meant to be the main gateway for users to search for blockchain-related information, checking transaction history, asset ownership recognition status and assets importation status.

HashFuture Token

Singapore HashFuture Foundation is the token issuing body. On the prerequisite of legal compliance in different jurisdictions, it will issue 50 billion HashCoin (HSC). HSC will be capped at a volume of 50 billion thereafter and will never have new supply. As the sole virtual currency circulating among Protocol layer, Technical layer and Application layer, it will have countless application scenarios and thus highly liquid.

Protocol layer: HSC is the authorizing instrument for use of HashModel protocol

In HashFuture eco-system, Foundation and its community will invite and gather professionals from different industries to formulate a set of standards for asset digitalization, ownership recognition and importing. The purpose is to make this set of rules acceptable in most countries, industries and communities. As HashFuture supports cross-blockchain transaction, users can obtain asset ownership rights in all blockchain by utilizing HashModel. This is achieved, say, when user consume HSC in an asset importation smart contract within HashFuture blockchain. The inventor of such smart contract can share a portion of HSC paid by users, this rewarding mechanism can motivate developers to design and release more add-ins.

Technical layer: HSC bridges digital assets across isolated blockchains

Relying on the HashModel protocol, users can pledge or lock their HSC in HashNode to build trust between buyer, seller and various blockchain communities. Demand on HSC will grow parallel with the increment in assets scale being digitalized and imported to HashFuture blockchain.

Application layer: HSC is the principal means of settlement in HashFuture's ecosystem

With the strategic partnership with HashWorld, HSC is designated as the only currency to rent advertisement banner in HashInsight, pay transaction fee on trading of HashAsset and pay administration charge on HashWallet withdrawal etc. Going forward, HashFuture will enable different industries to initiate their blockchain-related business activities via technical support, resource sharing and eco-system construction. Token so generated from external parties will be shared with HashFuture community members who held HSC via direct remittance.

HSC application illustrative scenario

Alex is a musician and he plans to sell his latest audio collection to fans via blockchain ownership recognition. He turns to Bob, an individual service provider of blockchain asset ownership recognition. Bob's qualification is obtained by pledging 100,000 HSC to the HashFuture community, therefore Bob is regarded as a HashNode. The audio asset digitalization protocol used by Bob is developed by a solicitor team led by Cindy, where the protocol can satisfy relevant regulations in China, Hong Kong and the US to ensure offline-online asset ownership consistency. No dispute has occurred in the past two years on such digitalized audio assets.

After Bob confirms Alex has the legitimate ownership over the audio collection, they signed on the asset digitalization and importation service agreement. Bob then upload relevant legal documentations in encrypted format to Hyperledger to ensure copyrights of the audio collection is transferred from Alex to HashNode owns by Bob's entity. Then Bob applies Cindy's audio digitalization protocol to create digital image of the audio collection in HashFuture blockchain, creation is effective via multiple digital signatures issued by different external parties. Bob then publish the digitalized audio collection on HashFuture asset trading platform, where sales of the collection is handled by pre-defined smart contract. HashFuture asset trading platform can support transaction in different cryptocurrencies and pricing models, warranting transparency, security, privacy and creditability on digital asset transactions.

David, a fan of Alex's music, is very interested on the audio collection published on HashFuture asset trading platform. He wants to purchase a copy to enjoy the music and at the same time enjoy potential appreciation on the audio equity. David checks on the HashModel protocol used and happily found that

the protocol has several successful cases recorded. Better still, the audio asset is processed in Bob's HashNode which has 100,000 HSC pledged. David decides to purchase the audio collection right away. The entire sale is executed on blockchain via pre-defined smart contract in a fraction of a second and minimal transaction cost. David pays ETH to Alex for a copy of the audio asset, simultaneously, certain number of HSC with lock-up period is paid to Bob and Cindy as agency fee.

Alex is seller and David is end user in this transaction. While Bob and Cindy are corner stone service provider in HashFuture eco-system who acts as HashNode service provider and HashModel protocol developer respectively. Bob and Cindy together render an easy-to-use solution for users like David who are not an expert in blockchain technology to purchase and invest in digitalized assets. HSC as the trusted medium in circulation, at one hand is being pledged by Bob to gain consent from community; at the other hand is being used by consumers like David to purchase digital assets. Naturally, when more digital assets are available on HashFuture trading platform, the need on HSC supply will grow accordingly. Holder of HSC can also participate in HashNode voting and give score on HashModel protocols etc. Everyone has a role to play in HashFuture's eco-system.
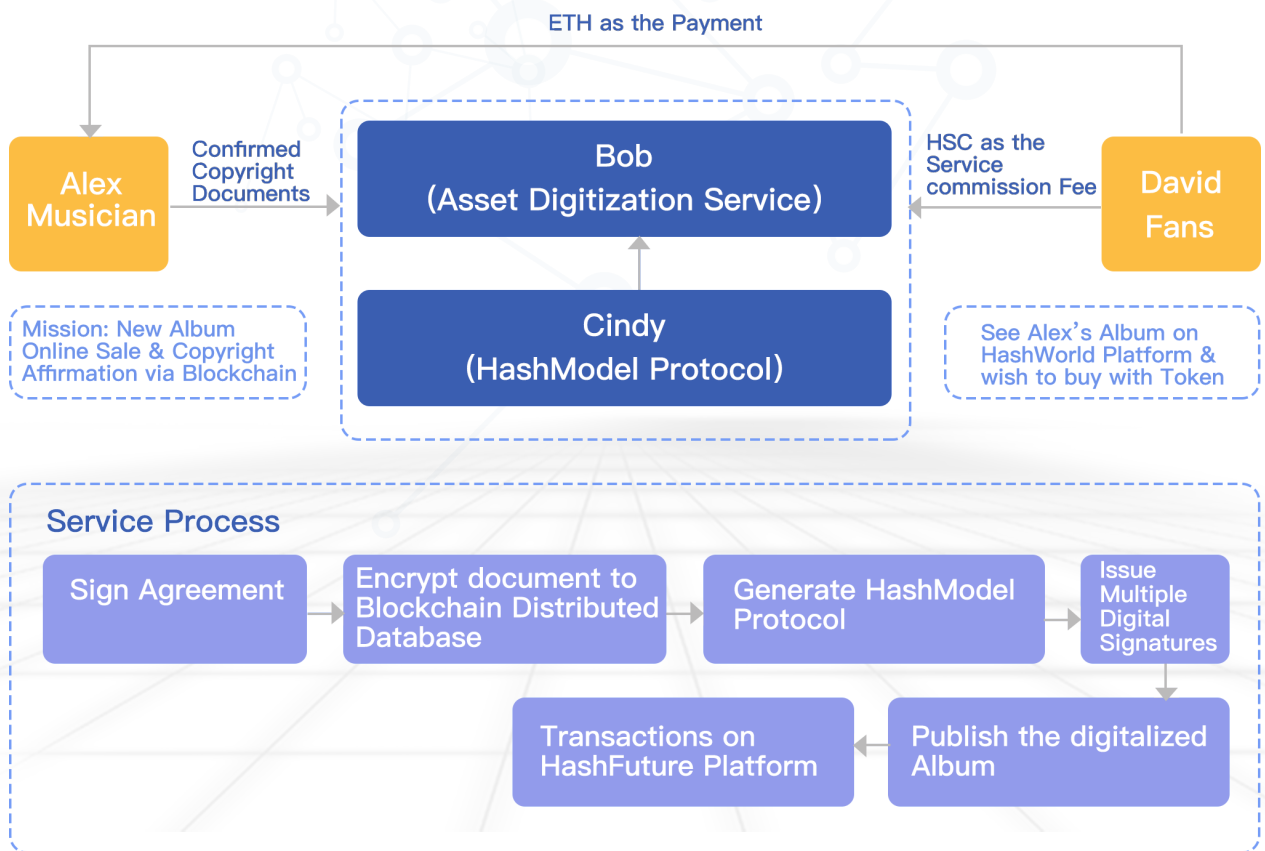

Figure 10: HSC Application Illustrative Scenario

HashFuture token allocation plan

HashFuture renders the following infrastructure to all dedicated developers and community members.

Total supply of HCS is 50 billion:

- PE and Exchange pre-sales: 30%, 1 year lock-up period for PE

- Founding team: 20%, 4 years lock-up period

- Foundation and Eco-system: 50% issue across 10 years, within which:

  - 10% for user motivation

  - 10% for service provider motivation

  - 10% for developer motivation

  - 20% for partnership, eco-system construction and investment fund

HashFuture's community governance

We, the founding team of HashFuture, hold our firm beliefs that blockchain technology and its protocols are meant to be a common wealth for all mankind. It must not be manipulated as a profiting tool as observed in various ICO scams. With this in mind, we established the Singapore HashFuture Foundation to support HashFuture development team no a non-profit making basis. We hope to keep the entire process transparent and fair, and welcome public scrutiny.

1) Operation vehicle

HashFuture Foundation is incorporated in Singapore with approval from the Accounting and Corporate Regulatory Authority (ACRC). It is subjected to regulation of Singapore's Companies Ordinance and is independently operated by the management committee. We decide to establish the Foundation in Singapore because it is well known for its stable legal system and financial environment. HashFuture Foundation, as a Nonprofit entity, is allowed to engage in charitable and private activities. It is straightly prohibited to participate in commercial or profit-seeking activities. Any earnings accumulated in the Foundation can only be retained to support future activities but cannot be distributed among members.

2) Governance structure

To ensure openness, fairness and transparency in the Foundation, the following layers of organizational structure are formulated:
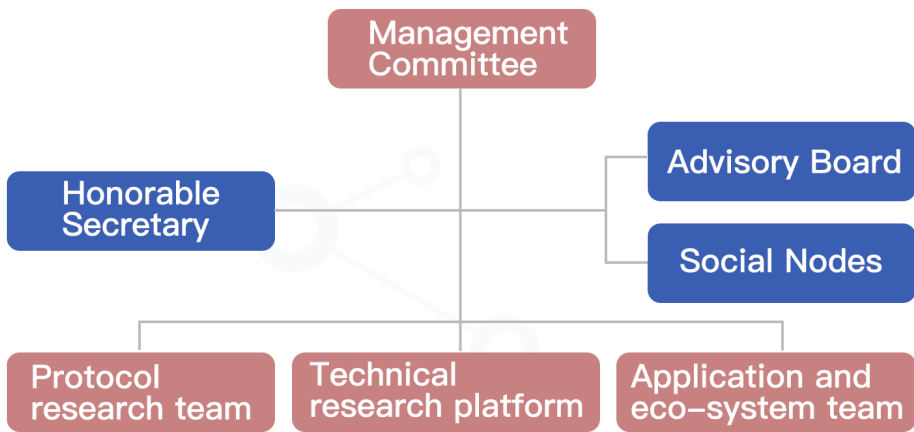
Figure 11: HashFuture Foundation Organization

a) Management committee

Management committee is the highest decision-making body in HashFuture Foundation. All committee members have equal rights and obligations. Members are responsible for discussion and approval of significant matters including formulation of development strategy, drafting annual plan and budget, and represent the Foundation to execute resolution on major events happening in HashFuture's eco-system.

b) Honorable secretary

The honorable secretary is elected among members of the management committee and is held responsible by the management committee. The honorable secretary organizes and executes all regulations and resolutions passed by the management committee. She is also responsible for daily operation of the Foundation and shall report progress to the Foundation regularly. The honorable secretary has the power to establish functional departments on a needed basis. She can also hire staffs, arrange researches and maintain HashFuture eco-system etc.

c) Advisory board

HashFuture would invite renounced politicians, academicians, entrepreneurs and social activists to join its advisory board.

Chief advisor: **Prof. Shou-cheng Zhang**

Lifetime professor of the Department of Physics, Electronic Engineering, and Applied Physics, Stanford University

Academician, National Academy of Sciences, the United States

Foreign Academician, Chinese Academy of Sciences

Founding director of Danhua Capital

d) Social nodes

The management committee will invite representatives from the HashFuture community to take part in the Foundation's governance to materialize the spirit of public sharing, involvement and ownership.

e) Protocol research team

Protocol research teams will be organized to address key questions on HashModel and HashNodes. Consensus mechanism and compliance with existing regulations are also area of focus of the research teams.

f) Technical research platform

The Foundation will pinpoint crucial issues on technical layer and infrastructure backbone to develop solutions on the technical research platform. Research results and solutions will be published regularly in the form of academic papers and open-sourced coding.

g) Application and eco-system team

The Foundation aims at promoting scenario-based blockchain applications, so that technology can create more values by tackling real life problems. The application and eco-system team is responsible for developing safe and simple API, educating developer community and liaising strategic partnerships. With participants interacting positively inside HashFuture eco-system, information asymmetry will be minimized and a vivid user community is sustained.

HashFuture development timeline

2018.2

Set Sail: the 1st product "HashWorld" released

2018.4

Elongation: Token system and wallet function completed

2018 Q3–Q4

Ecosystem: HashInsight, HashAssets, HashWallet released

2019

Consensus: Build up social consensus and protocol paradigm for asset digitization

2021

Sharing: Popularize the progress of asset digitization worldwide

2022

Standardization: A brand–new decentralized digital assets main chain

2018.1.1 2:43

Genesis: HashFuture Founded

2018.5

Sail Together: 1,000,000 users Achieved

2020

Connection: Popularize the standard platform for digital assets cross–chain circulation technology

2023

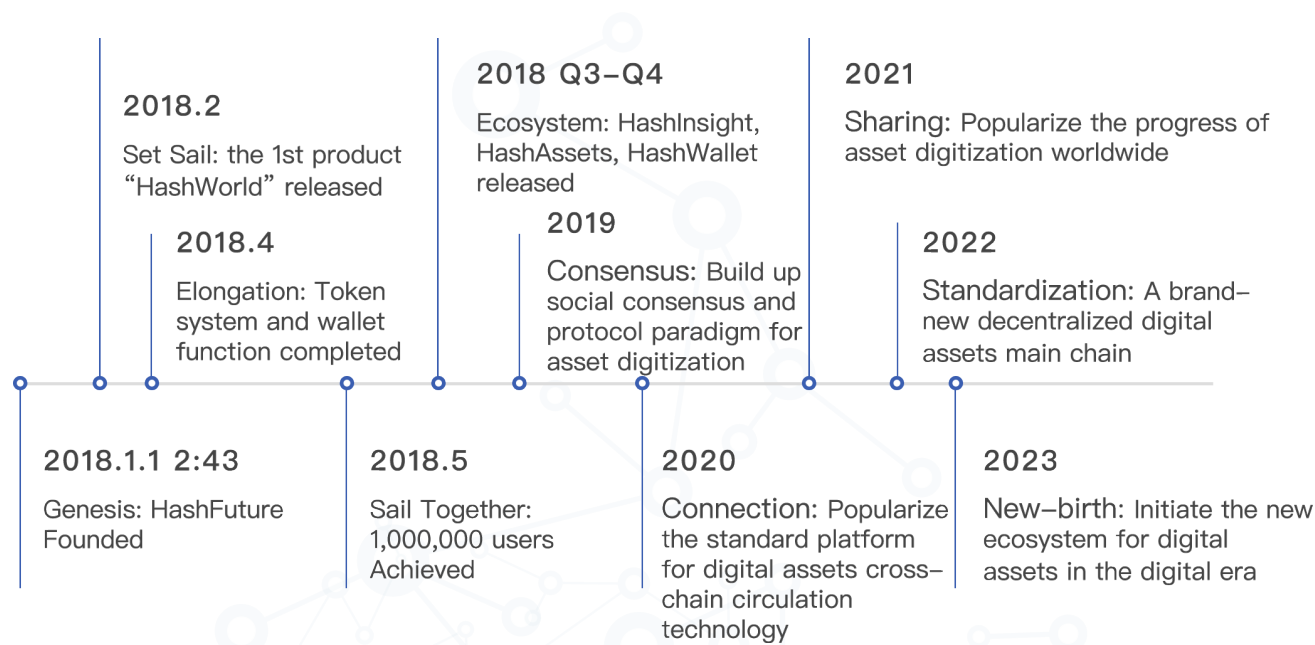New–birth: Initiate the new ecosystem for digital assets in the digital era

Figure 12: HashFuture Development Timeline

Disclaimer

HSC is not intended to constitute securities in any jurisdiction. This whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. The information set out in this whitepaper is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the purchase or acquisition of HSC and no virtual currency or other form of payment is to be accepted, on the basis of this whitepaper. You should not construe the contents of this whitepaper (or any part thereof) as legal, business, financial or tax advice. If you are in any doubt as to the action you should take, you should consult your legal, financial, tax or other professional adviser.

Participant of the HashFuture project acknowledge that she is of an age of majority to enter into agreement with HashFuture, meet all other eligibility and residency requirements, and are fully able and legally competent to enter into the terms, conditions, obligations, affirmations, representations, and warranties set forth herein and to abide by and comply herein.

The agreement so entered into between participant and HashFuture is legal, real and effective. All participants are voluntarily engaged in the HashFuture project and clearly understand project specifics and risk factors therein, and are willing to bear all results and consequences.

Any dispute shall be resolved under laws and regulations of Singapore.

HashFuture team would, on a best efforts basis, ensure information accuracy and completeness of this whitepaper. However, during project development updates may be made, inclusive but not limited to: protocol mechanism, token and its usage, token allocation plan etc. HashFuture team may communicate updates via announcement on website or publishing revised whitepaper (www.hashfuture.io). Participants are reminded that they should review their decision based on latest information available. HashFuture is not responsible nor liable for any damages or losses resulting from (i) reliance on information provided in whitepaper; (ii) incomplete information in whitepaper; and (iii) any acts induced by this whitepaper.

Despite HashFuture team would execute the project on a best efforts basis, there is chance that irresistible forces might occur and therefore HashFuture team cannot express a definite commitment.

Value of HSC is dependent on market demand and supply and is subjected to actual application usage. HSC may have zero value. HashFuture team, its agents, advisors and consultants DO NOT provide any

guarantee on HSC appreciation. All persons and parties involved in the purchase of HSC do so at their own risk. Any claims on guarantee of HSC appreciation are MISREPRESENTATION and are FRAUDULENT. Please contact the HashFuture team immediately if you come across any misrepresentation on the HashFuture project.

To the maximum extent permitted by the applicable law, HashFuture team does not accept any liability for any damage or loss, including loss of business, revenue, or profits (direct, indirect, punitive, actual, consequential, incidental, special, exemplary or otherwise) resulting from any form of participation in the HashFuture project.

HashFuture platform adheres to any regulations and voluntary disclosure requirements which are beneficial for blockchain industry development. By participating in the HashFuture project, participant is deemed to agree to all such regulations and disclosure requirements, and must provide accurate information for compliance purpose.

HashFuture platform does not perform due diligent check on participants. However, if any government bodies, industry watchdogs or subsequent risk management measure conducted by the HashFuture team discover any legal concerns on any participant, then HashFuture team has the rights to terminate any token agreement or redemption of token unliterally. HashFuture team does not accept any liability for any damage or loss arising from such occasion.

HashFuture team does not accept any liability for any damage or loss (direct, indirect, punitive, actual, consequential, incidental, special, exemplary or otherwise) including:

1. Trading loss resulting from user's operation;

2. Damages resulting from misunderstanding, negligence or inaccurate information;

3. Trading loss resulting from blockchain-based asset transaction.

Others

Official website: www.hashfuture.io

Email address: contact@hashfuture.io