MYKEY Self-sovereign Identity System
White Paper 1.0

Overview

MYKEY (mykey.org) is a self-sovereign identity system implemented on multiple public blockchains. The underlying protocol is called KEY ID. This white paper elaborates on design details of the asset management functionality, as well as briefly describes future development of MYKEY on two other aspects, namely social relationship and data protection. When it comes to asset management, MYKEY is a multi-chain wallet that gives users full control over their assets. Users are able to freeze and restore accounts when private keys get lost. MYKEY is also a building block of Web of Trust. Furthermore, in the context of Web 3.0, MYKEY turns data ownership back to users, protecting user privacy from the ground up.

1. Introduction

MYKEY is a self-sovereign identity system implemented on multiple public blockchains. It is also the first implementation based on the Key ID self-sovereign identity protocol. The App will be available in open source for both iOS and Android. One of the utility functions of the KEY token is to purchase ID names in the protocol. MYKEY Lab is responsible for developing the Key ID protocol. In return, MYKEY Lab receives an one-time donation of 10 billion KEY from Bihu Key Foundation. MYKEY Lab is a for-profit company that runs MYKEY App.

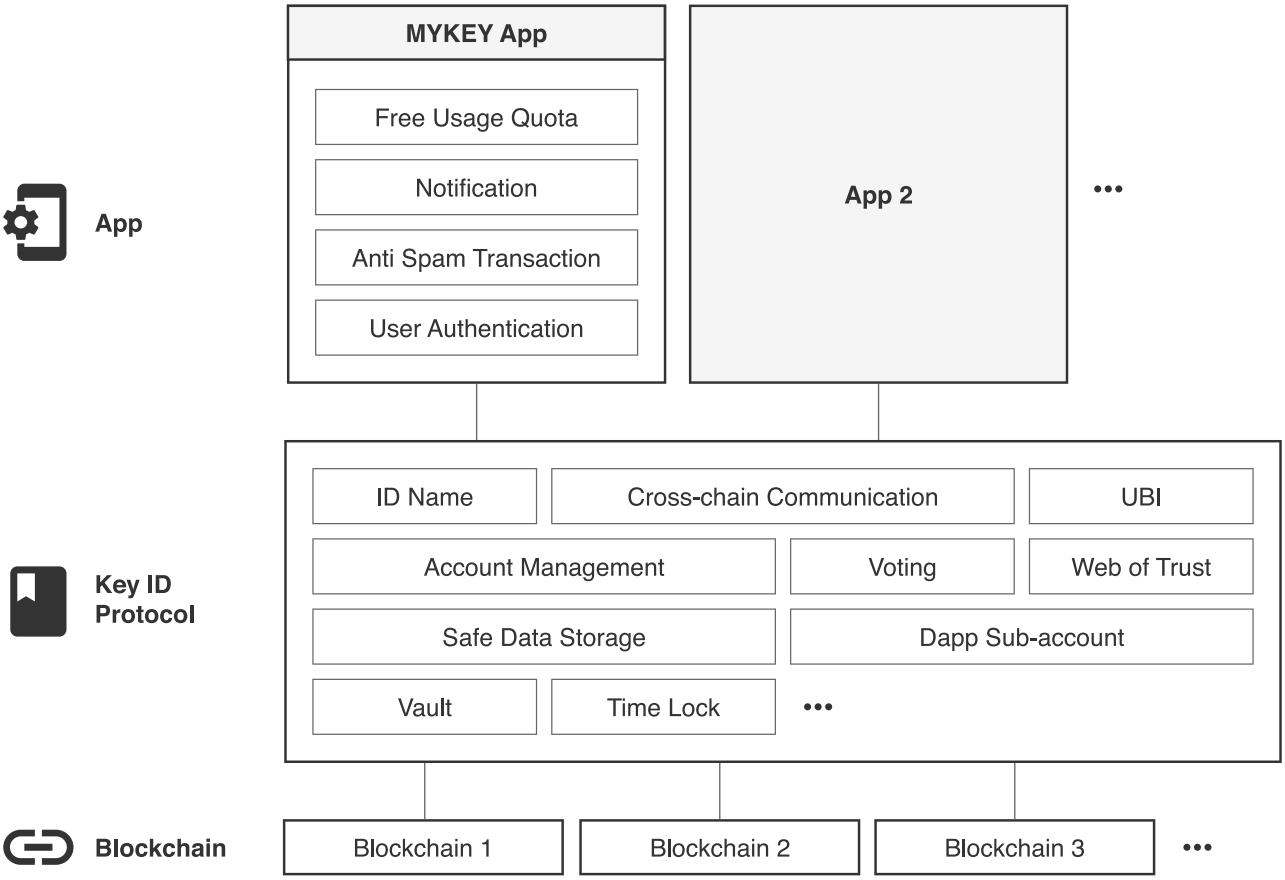

Fig. 1. Structure of MYKEY App and Key ID protocol.

MYKEY App means three things to an end user: multi-chain wallet, Web of Trust, and reliable data storage. MYKEY App provides wallet services on multiple public blockchains with the following features:

1. Universal ID Name,
2. Limited free use,
3. Comprehensive design on access control for enhanced account security,
4. Account recovery mechanism in the case of private key(s) loss,
5. Protocol upgradability,
6. Anti-spamming.

In a Web of Trust, each account consists of three components:

1. A universal and unique ID Name blessed with permanent ownership,
2. An identity account file;
3. A decentralized secure data enclave controlled by account smart contract.

Verifiable claim is another basic component of Web of Trust. In a Web of Trust, each identity account receives/sends many verifiable claims from/to other accounts. A well-knit Web of Trust is established via interlocking verifiable claims. Each verifiable claim can add and be linked to supporting documents, which are stored in decentralized data enclaves. These enclaves are accessible by other accounts only with owner's authorization.

Reliable data storage - Data stored in enclaves does not necessarily to be associated with any verifiable claim; instead, it can be stored independently, accessible by other accounts with account owner's consent. Files can also be made public by account owners. Data storage services and Web of Trust are based on the same infrastructure of decentralized storage, as well as on similar authorization mechanism.

Both the Web of Trust and data storage service rely on maturation of decentralized storage technologies. Therefore at the current stage, the development of these two products must be deferred into future.

2. Identity

What is an identity? An identity is a "shell" that hosts "me".

Identity has three attributes: social relationship, wealth, and data.

The attribute of social relationship indicates who you are in a social context. What roles does this identity occupy? It could be a son of farther a husband of wife, a boss of subordinates, and an activist member in some club. Social relationship defines "who I am". Should an identity have no social relationship at all, the very existence of such an identity simply does not matter.

Wealth attribute refers to the properties owned by an identity. For instance, a real estate property is registered under the name of an identity; a bank card belongs to somebody; one is entitled to use a leased computer. These are all wealth attributes of an identity.

Data attribute refers to data that is associated with an identity. For example, an identity conducted an air ticket purchase on some date; an identity owns 1000 photos; the entire shopping history on an e-commerce site is associated with an identity; past user activities on a social network site belong to an identity; personal data is recorded by wearable devices.

It is possible to re-organize one's identity on all three aspects in the context of Web of Trust, leveraging both blockchain technology and decentralized storage. Web of Trust enables aggregation of identity information that was originally scattered online and offline. It that sense, it builds a comprehensive "shell" and re-defines "me". Unlike what Web2.0 technologies enable, these powerful data are entirely under the control of identity owners and can only be accessed with owners' consent. An identity in Web of Trust is a virtual reflection of a real person in physical world. Although "I" will cease to exist after limited life span, the identity "shell" could be lasting for thousands of years, given enough storage fees are paid.

3. ID Wallet

3.1 Multi-chain Wallet

The MYKEY multi-chain wallet supports multiple smart contract platforms. Since each MYKEY account exists in the form of smart contract, MYKEY wallet can not support blockchains without smart contract features.

How to implement token migration across chains? The short answer is we cannot before cross-chain technologies get mature". As KEY is an ERC20 token on the Ethereum network, MYKEY has to address the issues of partial migration of KEY to other public blockchains. The quickest, maybe also the most effective way is as following: MYKEY Lab discloses its own KEY token holdings on the Ethereum blockchain, issues same amount of mapped tokens on other blockchains, and provides a service of 1:1 token conversion (excluding fees). Upon maturation of cross-chain technologies in the future, MYKEY Lab transitions back to a trustless manner of doing cross-chain interactions.

3.2 Identity

The Key ID protocol establishes a universal and unique ID Name for every user across all deployed blockchains. Identity accounts possess perpetual ownership and usage right over bound ID names. Because of the lack of cross-chain technology, a particular public chain needs to act as the root chain for ID names. The first blockchain on which the Key ID protocol is deployed will become the root chain, while ID name mapping will be established between other blockchains and the root chain.

One option to implement mapping is via "Staking + Challenge Period" mechanism. A same UUID (Universally Unique Identifier) will be assigned to a same user on all deployed blockchains, to indicate that these accounts all belong to the same user. Similarly, a user uses a same ID name on different blockchains. Unfortunately, UUID association is not authoritative proof when it comes to identifying a user, since anyone can mark a UUID to any newly-created identity account. An identity is established only after an ID name is bound to an account on the root chain.

In order to establish the mapping between identity account and ID name for the first time on a non-root chain, one needs to make sure that there is already a bondage on the root chain between an account with same UUID and such ID Name. Then one needs to stake a pre-specified amount of KEY tokens as deposit in order to initiate the identity mapping on the non-root chain. During the following “Challenge Period”, anyone can challenge the claim by staking the same amount of KEY tokens. If no challenger shows up before the “Challenge Period” ends, the identity mapping is successfully established on the non-root chain. If a challenger appears during the “Challenge Period”, the challenger will need to stake the same amount of KEY tokens. To further proceed, an arbitrator needs to verify two pieces of information: 1. whether the UUID and its corresponding ID name on the root chain are the same as those on the non-root chain; 2. whether both (A) the basic public keys associated with the account and (B) the account logic on the non-root are exactly the same as those on the root chain (“basic public keys” mean the original public key categories at the account creation). An arbitrator makes the verdict based on these two pieces of information. Loser loses his deposit, which is then distributed to winner, arbitrator, and MYKEY Lab, with split ratio undetermined yet. MYKEY Lab will build the infrastructure to carry out challenges.

How to elect arbitrators? If a non-root chain already has a mature oracle mechanism, this oracle will be used in challenges. Otherwise, a reliable oracle organization needs to be set up within the MYKEY community.

For identity accounts and ID names that are already bound on a non-root chain, one can still change them via “Staking + Challenge Period” mechanism so as to correct any possible mistakes. However, the threshold to change will be set much higher than that of initial setup, so is the KEY token amount that is required for such a change, and the challenge period would also be much longer. Lastly, there is no limit to the number of times that one can call for challenges.

The naming convention for an ID name:

1. An ID name can contain 1-63 characters;
2. Allowed characters: 26 English alphabets (a-z) in both upper and lower case; numbers 0-9 and the hyphen “-“;
3. ID names are case-insensitive;
4. ID names cannot start with or end with a hyphen “-“.

Though a MYKEY identity account can own multiple ID names, an ID name becomes permanent and irrevocable once it is bound to a MYKEY identity account. A MYKEY account is only allowed to be bound once, namely be bound to one ID name. Any unbound ID names are transferable to others.

To prevent ID name squatting, all ID names will be released gradually through auctions. Because of the openness of the KEY ID protocol, auction participation is not limited to MYKEY accounts, but open to all. To be specific, all blockchain accounts of the root chain equally participate in all auctions. Proceeds from auctions go to MYKEY Lab. Rules for auctions are as follows:

1. ID Name amounts released schedule:
    - Single-character ID names: 1 ID name every 120 days;
    - 2-character ID names: 1 ID name every 7 days;

- 3-character ID names: 5 ID names every day;
- 4-character ID names: 125 ID names every day;
- 5-character ID names: 3000 ID names every day;
- 6-character ID names: 85000 ID names every day;
- ID names with 7 characters or more: no cap.

2. Every ID name requires a minimum payment of 0.1 KEY;
3. Bidding price increments at least 10% higher than the previous bid;
4. An ID name auction can be settled, only if there is no new higher bid within 24 hours;
5. Within each category of ID names, the ones with highest bidding price get settled first. When the daily quota of an category exhausts, unsettled bids postpone to the next day. These postponed bids do not enjoy any priority in terms of settlement.
6. Any unsettled ID names can be bid.

3.3 Limited Free Use

Note that the feature of "free use" is not an inherent component of Key ID protocol, but rather a perk provided by MYKEY App, which happens to the first instance of KEY ID protocol.

While people are long used to the FREE mentality on the internet, it is an inevitable pain to pay for blockchain usage as fees are inherent part of public chains in order to prevent spam attack. Some seemingly "free" blockchains charge fees via the time value of tokens, which apparently defeats the "free" claim.

Fees introduce friction, and raise bars for user participation. To find a smoother path for mass adoption, MYKEY provides certain amount of free usage on all deployed public blockchains. When registering a MYKEY account, one can choose to complete the verification to get a free account and some free usage quota. MYKEY Lab does not keep any identifying user information once the verification is complete. It only stores the hash of (name + documentation type + documentation number + random number) to prevent abuse of repeated free account opening, meanwhile protecting user privacy.

Free usage quota is denominated in KeyPoint (KP), which is non-transferable. On book value, 1KP = 1USD. In early days, each and every user who passes the verification receives a certain amount of KPs. Additional KPs can also be granted based on user behavior.

To those who do not complete verification, the blockchain fees are on their own. They can purchase KPs for usage.

3.4 Account Security

The security of a MYKEY account is warranted by a few mechanisms. First, MYKEY App as an open source project is subject to comprehensive community scrutiny. Bounties will be offered to identify potential code vulnerabilities.

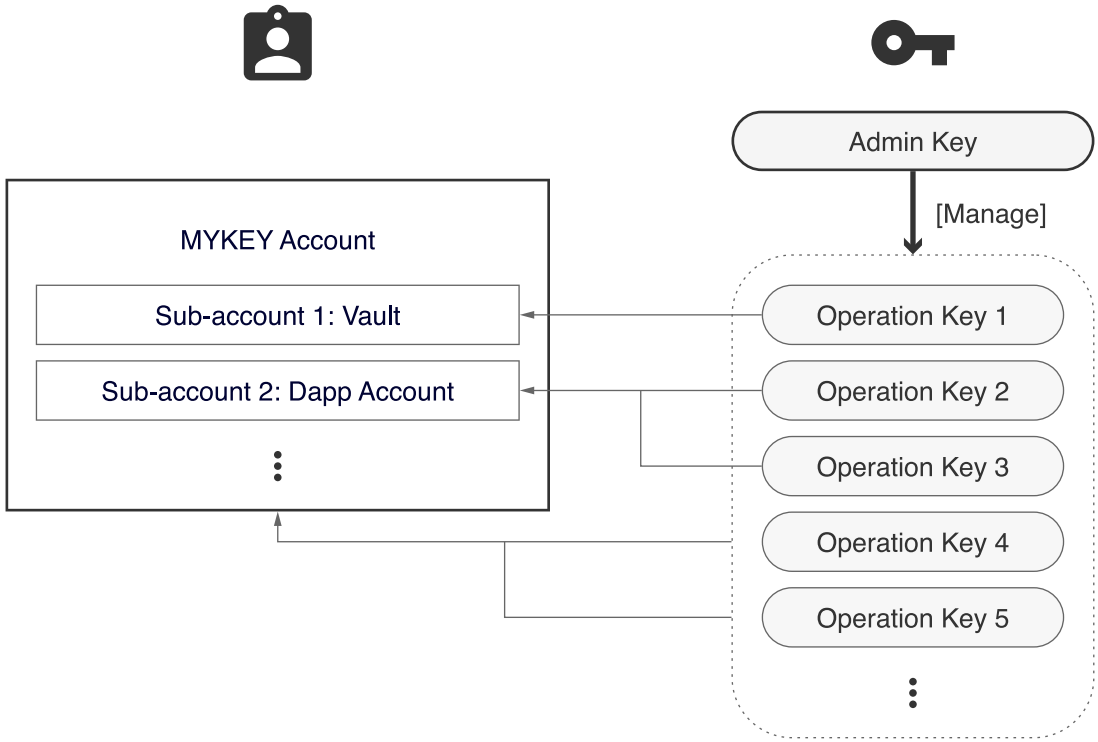

Fig. 2. MYKEY account system and private keys authorization structure

Secondly, as shown in Fig. 2, the design principle of MYKEY is based on balancing access control mechanisms, joined with time-delay mechanisms for further security. Therefore, it avoids one-point-failure vulnerabilities. Access authorizations are jointly controlled by “Admin Private Key” and “Operation Private Keys” as below:

1. **Admin private key.** An admin private key possesses the highest authority of the account. It must be held **solely and independently** by the owner, and shall not be shared with anyone in any circumstances. The admin private key is not stored within the device where the MYKEY app is installed. Instead, MYKEY App prompts the user with 12-word mnemonics to be stored offline on paper. These 12-word mnemonics can be replaced with hardwares in the future. An admin private key is able to freeze and replace operation private keys, as well as replace itself. However, it is not capable of direct account authorizations, such as asset transfer. Its authoritations are as follows:

A. To unilaterally freeze an account’s operation private key(s), effective immediately.
B. To unilaterally unfreeze an account’s operation private key(s), effective with a 7-day delay; or effective immediately if co-authorized by emergency contacts.
C. To unilaterally replace an account’s operation private key(s), effective with a 7-day delay; or effective immediately if co-authorized by emergency contacts.
D. To unilaterally replace itself, effective with a 21-day delay; or effective immediately if co-authorized by emergency contacts.
E. To unilaterally revoke waiting-to-be-effective activities of replacing admin private key, replacing operation private key(s), and unfreezing operation private key(s), effective immediately.
F. To unilaterally add/remove emergency contacts, effective with a 21-day delay.
G. To add a category of operation private keys, effective immediately.

2. **Operation private key.** A category of operation private key(s) controls the authorization of a specific function. Each and every function can only be exclusively authorized through a specific category.

2-1. **Responding private key** of being an emergency contract. Each MYKEY account can become other MYKEY accounts' emergency contact, which means that each and every user can set up trusted individual(s) or institution(s) as his/her emergency contact(s). MYKEY Lab acts as MYKEY account's initial default emergency contact. Users can add/remove emergency contact(s), with a limit of minimum one emergency contact and maximum of six. This limit is imposed by MYKEY App, other than the Key ID protocol. Emergency contacts are able to assist an account owner in the case of emergencies. An action is approved and executed when 60% or more of emergency contacts approve. The authorizations of a responding private key are as follows:

A. To assist with being-assisted person's admin private key in the case of unfreezing operation private key(s), effective immediately.
B. To assist with being-assisted person's admin private key in the case of replacing admin private key, effective immediately.
C. To assist with being-assisted person's admin private key in the case of replacing operation private key(s), effective immediately.
D. To unilaterally replace the admin private key of being-assisted person, effective with a 30-day delay.

2-2. **Asset management private key.** The asset management private key is able to manage all assets under the MYKEY main account, such as asset transfer or collateralization. This particular private key has no authority over these assets that stay in those special-purpose-sub-accounts of MYKEY.

2-3. **Operation private keys for special-purpose-sub-accounts**, such as savings accounts, and sub-accounts for external applications, etc.

2-4. **Private key for login.** To authorize the login operations in various external applications using a MYKEY account.

2-5. **Private key for vote.** To vote on proposals with MYKEY account.

2-6. **Operation private key for verifiable claims.** A MYKEY account is an instance of Key ID. As the fundamental building block of the self-sovereign identity protocol, a KEY ID issues verifiable claims to other Key IDs.

With the above authorization settings, an account can be recovered in the following scenarios given that emergency contact(s) remains credible:

1. Forget the password of MYKEY App.
2. Loss of device(s), such as mobile phone(s).
3. An operation private key is leaked.
4. The admin private key is lost.
5. The admin private key is leaked.
6. Loss of device(s) and the admin private key simultaneously.
7. Severe accidents occur to users, which lead to long-term disappearance or death.

Users are not able to recover accounts in only one scenario: the admin private key is both leaked **and** lost at the same time. In this case, the system can't literally distinguish the person who currently holds the private key from the supposed account owner. In other words, the ultimate criteria for the system to recognize a rightful owner is with the exclusive possession of admin private key. For this reason, MYKEY App will kindly remind all users to make at least 2 copies of mnemonic words in the initial setup, and to store them in different locations that are known to nobody else. So even if someone accidentally obtains one of the mnemonic copies, one still has other backup(s).

Later, MYKEY will consider services tailored for institutions, and further customize authorization settings for these institutional clients.

3.5 Upgradable Protocol

Upgradeability is of great significance for the long-term prosperity of a protocol. The Key ID self-sovereign identity protocol will evolve along with maturation of the underlying technologies, such as decentralized storage and cross-chain technologies, to better meet users' need.

There is inherent contradiction between the protocol's upgradeability and trustlessness. A graceful resolution to this contradiction must include reaching out to our broad community to get an overwhelming consensus towards upgrade, meanwhile providing those who oppose with rights to opt out. New code must pass a thorough community audit with sufficient time given, aided with bounty programs for code vulnerability detection. Meanwhile, a pending period is pre-specified in the smart contracts that regulate protocol upgrade. This pending period cannot be skipped, and therefore users will have time to opt out. The pending period is set to be 4 days in the beginning, and is expected to gradually increase as the KEY ID protocol matures.

The protocol upgrade is triggered by a multisig account that is under control of MYKEY Lab. Tokenization of MYKEY Lab described in Section 6 certainly helps to form broader community consensus before protocol upgrade.

3.6 Anti-spamming

Spam transaction filtering is one of the great MYKEY features that are not part of the protocol layer. MYKEY App implements a smart, dynamically-adapting mechanism to filter spam transactions, and thus achieve better user experiences.

4. Web of Trust

More details on Web of Trust will be given in future versions of this white paper. This version gives only guiding introductions.

Web of Trust consists of two parts: identity accounts and verifiable claims. An identity account complies with the Key ID self-sovereign protocol, as MYKEY is one of implementations of Key ID. A verifiable claim is an assertion made by one identity account to another. For example, identity account A can state that the age of identity account B is equal to or greater than 21. The attribute of verifiability stems from the distributed ledger technologies, as relevant details (subject, object, time, content) cannot be tampered secretly without anyone noticing.

Identity accounts are nodes of Web of Trust, whereas verifiable claims serve as linkages among these nodes. This allows for fact-checks across many independent identity accounts, thus forming a humongously large Web of Trust. It is the interconnecting structure of Web of Trust that makes identity verification highly effective and reliable, leading to an final end of fake identities and false claims. Trust can be established and relayed in hierarchical structures (blue links shown in Fig.3) as well as in free-style structures (green links shown in Fig.3).

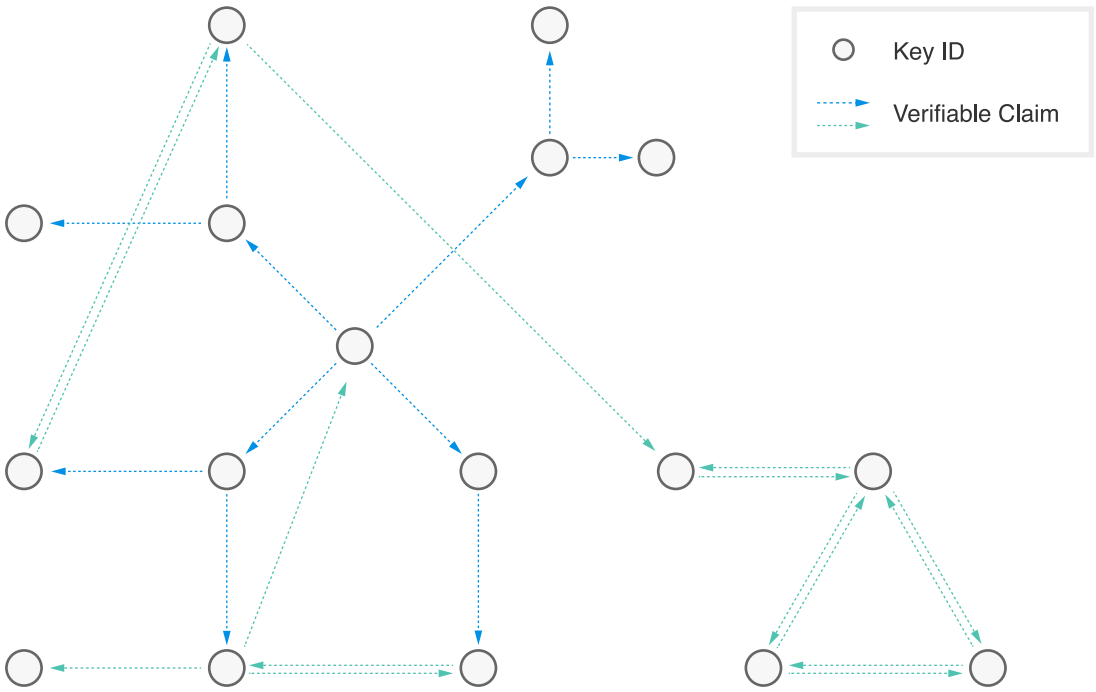

Fig. 3. An schematics of Web of Trust.

From a technological perspective, an identity account consists of three parts: (A) an ID name, (B) an identity file, (C) a secure data enclave based on decentralized storage technologies, and fully controlled by identity smart contract. ID names are already explained in section 3.2. An identity file consists of attribute descriptions of an identity account. For more details, please see to the link. A secure data enclave is a special decentralized data storage container that is under full control of account smart contract. It can be used for storing both public and private information about an identity account. The architecture of the secure data enclave and its development pace depend on the progresses that decentralized storage technologies

make. Until then, a mid-ground solution seems necessary.

The promises that a Web of Trust gives include but are not limited to the following:

1. Address issues that are caused by fake news, false informations, and frauds, which take advantage of video/audio synthesis technologies (i.e. DeepFake).
2. A more comprehensive and more efficient personal credit-scoring system that hopes to reduce frictions caused by the lack of trust (i.e. to prove my mom is indeed my mom).
3. Open a whole new window for innovative ways of collaboration based on Web of Trust.

5. Reliable Data Storage

This part will be elaborated in upcoming versions of this whitepaper. This version depicts only basic ideas.

Secure data enclave, mentioned in previous sections, is not only a fundamental component of Web of Trust, but also plays an important role in other identity-related areas. Therefore, it justifies a dedicated section.

5.1 Privacy in Web of Trust

Since information on public blockchains is available for all, it is inappropriate to store private data on-chain. Full details of a verifiable claim is not suitable for on-chain storage. Instead, it shall be stored in secure data enclaves controlled by identity accounts. Only a cryptographic fingerprint is published on public chains to achieve verifiability. The fingerprint can be some form of hash tree root, such as root of Merkle Tree.

5.2 Full Record of Personal Data

Based on the decentralized storage technology, the secure data enclave is under full control of account smart contract. That means that the owner of the identity account fully controls the data in the enclave, and no one else gets access to the data without the owner's consent. As a result, it is safe for the owner to store his/her highly sensitive data in the enclave. For example,

1. Personal health data,
2. Full record of online activities,
3. Wills,
4. Data recorded by wearable devices.

Data can be shared with other identity accounts with the owner's consent, or be made completely public. Thanks to the programmability from smart contracts, it is feasible to pre-program the ways how data will be shared. For example, a will in an enclave can be programmed in such a way that it shares with certain accounts after the owner's identity account remains inactive for a prolonged period of time. It is also possible to make all the data in an enclave completely public in the 50th year following the death of an identity owner. Thanks to the extreme reliability brought about by decentralized storage technologies, it is even possible to

preserve data for thousands of years, given enough fees are paid.

5.3 Decentralized Applications

Data from decentralized applications (Dapps) can be stored partially or fully on decentralized storage. Thus, access to corresponding data requires authorization from owner accounts. Some data from Dapps can also be stored in the enclave of users. Dapps and identity accounts have their own individual secure data enclaves. Such dual data storage structure provides high flexibility to Dapp development. For instance, in an election Dapp, zero-knowledge proofs can be used to protect privacy without revealing full voting details. Instead, these full details are kept private in the enclave of users.

6. Tokenization of MYKEY Lab

Disclaimer: contents in this section should not be interpreted as commitments. Whether, when, and in what ways MYKEY Lab will be tokenized, is at the sole discretion of the shareholders and management team members of MYKEY Lab.

Centralization is undeniably more efficient than decentralization. In the early period of rapid development, a project usually benefits from strong driving forces of a centralized team. Despite the centralized start of MYKEY App, blessed with its great hope of becoming a fundamental infrastructure of human societies, MYKEY pictures itself ultimately as a public App, taken over by the community, owned and governed by all.

After tokenization, MYKEY Lab will cease to be the governing body of MYKEY, but a mere nominal entity. Instead, a token called Governance Token (GT) for the moment will be entitled with decision-making power for both MYKEY App and Key ID protocol. Most of the profits earned by MYKEY Lab will be kept in the form of GT after tokenization, whose allocation will be determined by some form of token vote.

Distribution of GT. The total amount of GTs is 100 billion, with 40% be allocated to users, 20% to the operation & promotion pool, 25% to the shareholders of MYKEY Lab, and 15% to the to-be-established Key ID Foundation. The allocations of both 25% and 15% will be released linearly over a period of four years. This process will be regulated by smart contracts that are established during the tokenization process.

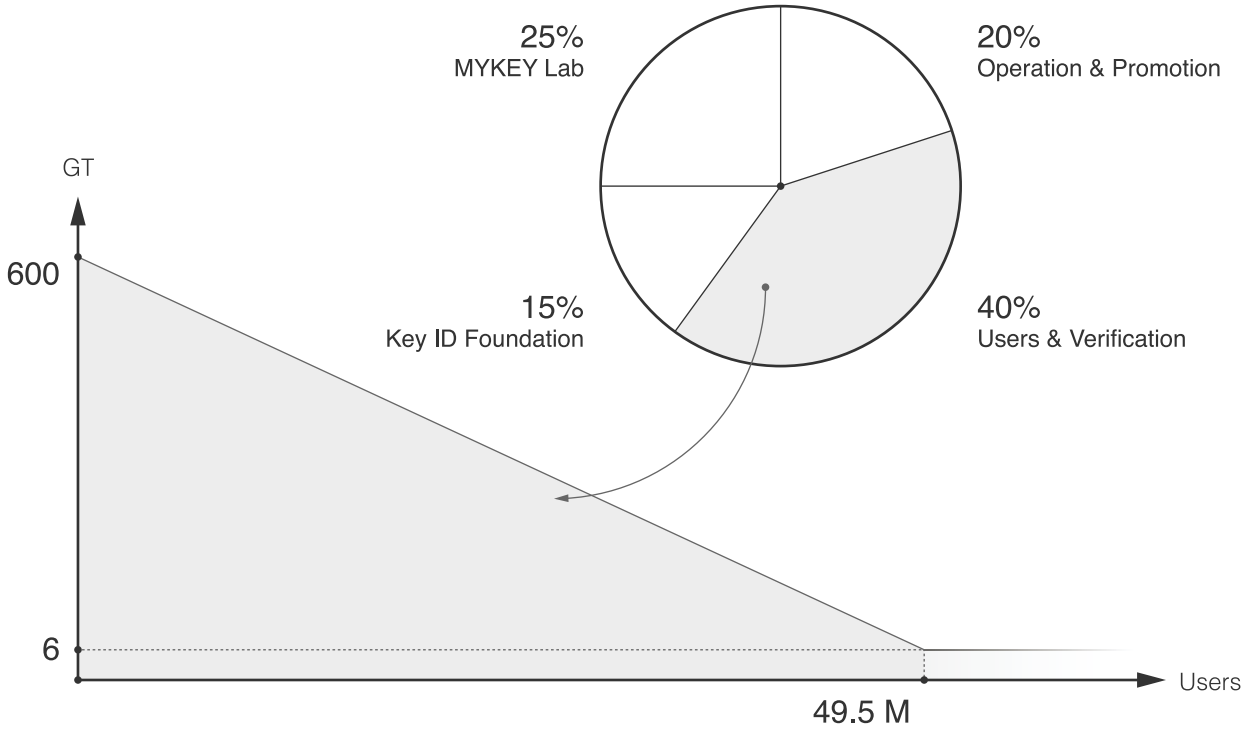

Fig 4. Distribution of GT

The distribution plan for the user pool of 40 billion GTs:

1. For the 1st-10000th users who pass identity verification, each gets 600 GTs.
2. For the 10001st-20000th users who pass identity verification, each gets (600-1*0.12) GTs.
3. For the 20001st-30000th users who pass identity verification, each gets (600-2*0.12) GTs.
4. And so on so forth, until the reward linearly reduces to 6 GTs per user. Every user who passes identity verification will obtain 6 GTs indefinitely till the depletion of the user pool.
5. The plan above suggests an average amount for each user. Fine adjustments can be made according to market feedbacks. For example, set aside 20% for referral rewards.
6. All costs incurred to the identity verifications are covered by the user pool.

After tokenization, MYKEY community will be mainly governed by representative democracy, complemented by necessary direct and/or liquid democracy. To be specific, a committee elected by all GT holders once every four years will run the MYKEY Lab and the newly-established Key ID Foundation. MYKEY Lab appoints the first interim committee after tokenization for a two-year term. This interim committee is responsible for drawing up the “MYKEY Community Consensus Convention”, which will act as the long-lasting guiding principles for the governance of MYKEY community. The MYKEY Community Consensus Convention defines the committee's rights, responsibilities, boundaries of interests, and rules of changing rules. In principle, the community can revise any rules through GT referendum, as long as the GT voting participation rate exceeds certain percentage and the score of consent exceeds 2/3 (note: the score does not necessarily equal to the ratio of votes, because the scoring algorithm is not limited to token votes). This approach hopes to keep the governance both flexible and evolving. It is worth to mentionning that only the locked GTs are counted as valid ballots.