Abstract

PoS (Proof of Stake) world adopted Stake model as a safety feature, weighing its players by, not computing power as its PoW (Proof of Work) counterpart, but how many tokens they are staking—solving extravagant computing power arms race for the right to produce. On the strength of that, it was making its debut while claiming its superiority over PoW. Any PoS system is underpinned by the stakability of its token, as an approach to keep it democratic enough. It is, in a way, solving the centralization problem of computing power in PoW. This mechanism, however, puts "Stake" itself at stake. Whereas, relevant solutions are not perfect enough so far, some hurting the interests of token holders, some others depreciating the system as a whole. On the one end of PoS spectrum, almost all field tests of it are integrating incentives for a higher Stake ratio from a safety aspect. On the other end, they also are binding stake tokens to a lock period to prevent potential attacks from a bulky token staker. In the middle is a paradox between the safety of mainnet and the liquidity of tokens. That is to say, a system that locks all tokens staked is an extremely safe one, but its value growth is pushed to the brink due to zero token liquidity. Therefore, we are determined to create a decentralized protocol that provides liquidity, that can make locked assets circulate freely. In this way, Liquidity is guaranteed by issuing rToken (reward Token) while the original tokens are staked to the chain remain comparatively static to keep the system safe.

I.Background

PoS was debuted in 2011 by Quantum Mechanic on Bitcointalk Forum. The system creatively replaces computing power weight by token weight in Block Producer elections. Token holders can claim its run for BPs to the system by staking their tokens, while the system selects BPs through random algorithm. Those selected will be responsible for packing, verifying of transactions and prolonging the chain. As a late-comer to the game, PoS drew on the experience of PoW with regards to consensus, elections, packing, validation and so forth. As technology advances, PoS is steering the development of blockchain world in performance, capacity and sustainability. 2019 and the following year will be seeing, with excitement, the landing of second-generation PoS 1 consensus as projects like Cardano, Tezos, Cosmos, and Polkadot will soon launch the mainnet, making them the touchstone of PoS consensus in the new era.

Stake model in PoS overturned computing power weight, integrating the right of possession with that of mining. So that the token holders can participate in the system consensus just through staking. During the whole process, the token holders only have to run servers of certain standards or delegate to professional validators (After 2015, all mainstream PoS projects started integrating delegating mechanism to enhance the staking ratio of tokens, thus making the system safer). Moreover, random election solves the problem of squandering computing power brought about by mining competitions. At the same time, a new blockchain relationship is created—holders are miners, blowing a new wind to the public chain world.

Incentives, no matter when it comes to PoW or PoS, are integrated in order to encourage engagement in nodes operation. Right before the launch of a mainnet adopting PoS consensus, the system will strengthen the incentives to guarantee that enough tokens will be staked. Therefore, more coins that are initially distributed will be locked to step up systemic safety. As Arthur, the founder of Tezos, wrote in that project'_s whitepaper: the preliminary

incentives must be high enough. This is of paramount importance for a safe launch of mainnet. Stakers must bear certain time and opportunity costs (2). If the incentives fall short, the mainnet will bear grave safety threats. Another example, Cosmos wrote floating annual rate that is as high as 7%~20% to its codes to motivate staking while their mainnet was launching.

Lock period is an important feature that sets PoS apart from PoW consensus. In Stake model, the system has stability requirements for tokens staked, which is used to prevent long-range attacks: Nothing at stake. There is also a problem of computational fragmentation. The tokens that have been staked are locked by the system for a certain period(3). Although the token holders can initiate the unlock at any time, but the tokens will still be untradable during the unlocking period. That is to say, holders still can't dodge the risk of value fluctuations of the token at that phase. This is underlied by the contradiction between Token Stake security and token liquidity.

The paradox, to a large extent, causes problems in both ways. Many people are too afraid to stake, and the system will be in jeopardy as a result. This is a slippery slope, for a small nexus is seizes most reward fruits while the system still remains highly risky. For some PoS consensus projects that have already launched, the Stake rate is about 40%. As for those star projects, the number is generally around 50%~60%, up to 80%, less-known ones only about 20%. In theory, the most satisfying Stake rate, from a safety aspect, should be 100%, but this is often unrealistic. In addition, the 100% Stake rate means that the liquidity of the token is 0. For many projects with a vision of creating a blockchain OS (operating system), the liquidity of the token plays a significant role in underpinning the operation and value of the system. So, the impact of zero liquidity is almost entirely negative. At present, PoS world has not reached an agreement on a reasonable Stake rate. Or, maybe we should put it this way—it is impossible to reach an agreement because of testing a distributed network with a simulated environment is hardly possible.

Stafi provides a secured solution to address the conflict between the mainnet security and the token liquidity in the Staking model. The token holder obtains bonded assets of equivalent value to the tokens by Staking in exchange for equivalent rTokens. For example, if a user stakes 1 XTZ, he will obtain rXTZ (reward XTZ) that is equivalent to the original token. rXTZ represents regular yields of tokens and the ownership of XTZ on the original chain. At the same time, rXTZ can be traded on the bonded assets market based on the Stafi protocol. Different to XTZ that is staked and locked on the original chain, tradable rXTZ has no lock period, but still keeps generating returns. As a result, holders of rXTZ no longer need to bear the risk of volatility and make timely judgments on market conditions. The Stafi protocol gives holders more rights. Due to financial motives, a holder will join the Stake contract for Staking for the risks no longer exist. This will serve as an adrenalin to Stake rate. Theoretically, projects that are decentralized enough will increase the Stake rate to over 90% (missing tokens not considered) while at the same time maintaining the liquidity over 90% with the help of Stafi protocol.

II. Existing Work—Unleashing Liquidity

The pre-existing ways of doing this are scarce, which can be categorized into decentralized and centralized ones.

A centralized token circulation model is often endorsed by a third party, which obtains the ownership of tokens by collecting them from holders, then conduct Stake in an intensive way. Tokens that are staked will be used to produce blocks through a node, thus being rewarded. When the third party reaps enough tokens, it will be well-positioned to issue alternative tokens to its customers. Then, it can also launch a trading pair with that issued token on one end, in collaboration with a centralized exchange; or even create a trading pair at any decentralized exchange. Holders of that token can trade the ownership (also redemption right and income right) of the original token, without redeeming tokens on the primary chain. In this way, the liquidity of Stake tokens are, to some extent, boosted. There are side effects, though. This model is hardly possible without the trust of token holders in the endorsement of a third party and in the authenticity of its redemption and income right. Trust alone is insufficient still. Holders must take into consideration the third party's capability of guaranteeing the trading depth of the trading pair with the token. This capability is determined by various factors, of which an important one is third party's deep pocket filled with Stake tokens. Small-scale third party is entitled to the right to issue the bonded assets. If the power is wielded, however, few may respond. And this way of unleashing liquidity exists in name only. On the other hand, if massive alternative tokens are minted by one single bulky third party, another risk may underlie—centralization, exposing that party to the attacks by hackers. Users' assets may also bear grave loss. Similar attacks can be found in the history of attacks to centralized exchanges, which was happening frequently. Set security issues apart, this approach runs in oppositions to the very decentralized spirit in blockchain world.

Another centralized approach lies in the cooperation between a project party (Developers, or Devs) and a centralized exchange. Assets that are staked are endorsed by the project party for that exchange. Or, Devs may even delegate custody of locked Stake tokens to the exchange (provided that the ownership to the tokens that are staked is explicitly held by Devs when Stake was designed). Endorsed by Devs, the exchange can issue an alternative token and create multiple trading pairs derived from this token to ensure the liquidity of Stake tokens. Meanwhile, it supports all redemption actions for Stake tokens on the primary chain by that token. But the exchange cannot be bypassed. The problem is that Devs change the ownership relations of assets and misappropriate assets arbitrarily. When the ownership of tokens is handed by the exchange, problems like covert deals or embezzlement may happen. There are examples in the theft of exchange in the history. In a nutshell, the aforesaid two approaches are both completely deviated from the decentralized spirit of the blockchain.

The third approach is that Devs modify the underlying protocol in order to obtain Liquid Token after staking (which can be called PBLT, Project-Base Liquid Token). Users can trade PBLT without waiting for the unlocking time of the Staking Token, solving the security threat brought by frequent unstake and bringing convenience to users. The advantage of this solution lies in PBLT as an alternative token endorsed by a system-level entity to guarantee security. And at the same time, the rights entitled to PBLT is recognized by the entire consensus. However, the problem is that most of the public chains that have been launched are still maintaining a relatively neutral attitude, for it may be difficult to directly modify the underlying layer, and the open community development process will be strained. For PoS Token holders, this is not an all-round solution. At present, only Cosmos and Near Protocol have put forward their own ideas. The holders of other assets cannot solve their locking problems like this.

Stafi protocol is meant to establish a Staking Contract at the upper level, so that the holder can initiate a Stake through the designated Contract, and at the same time obtain rTokens, an

alternative token. The rTokens can trade their possessions at the bonded assets exchange built on the application layer. The holder's Stake process and the rToken issuance process are both automatically executed by the contract code. There is no need for any third party endorsement, and the user holding the Stake token can initiate Stake or redeem at any time, the contract will be automatically executed once the validation is passed. Except for the absence of third-party intervention, the entire rToken distribution rights are given back to the original chain token holders. Further, holders can issue the value-bearing bonded assets of the corresponding value, which is similar to the current method of asset securitization. The biggest difference is that it is each and every individual, but not institutions, who issues bonded assets. The meaning of individual issuance is to resist volatility. Therefore, in theory, this decentralized method should better motivate the original chain holder to obtain rTokens. To this end, the number of rTokens on the market will also become sufficient to prop up the bonned assets bond trading market. Meanwhile, this decentralized model will reversely stimulate the trading of bonded assets, thereby reducing the spot transactions. As a result, the great picture of mass issuance and trading of bonded assets will be finally realized.

Mass issuance of rTokens is endorsed by Stake Assets, and Stake Assets is endorsed by the public chain/function behind its model. At present, the Stake model has not been abused, which guarantees the quality of Stake assets. But the problem/risk of this kind of bonded asset is that the regular income of this Stake asset is highly dependent on Token. Although the holder can continue to earn income through Stake, this income expectation to legal currency is still fluctuating, which causes inconsistent expectations of rToken trading in the trading market. Leverage may fill the market in great numbers, which brings more opportunities and possibilities to the creation of decentralized bonded assets trading on Stafi. When a large number of PoS consensus projects are launched on the main network from 2019 to 2020, the Stake assets will proliferate and the transactions will become more frequent. When the holder of the currency is also the debtor, tokens that are staked will serve as the collateral. And the redemption right will be shift as the collateral is traded. These relations are all stipulated by smart contracts, not by centralized companies or institutions, and this stands Stafi, a decentralized protocol, out among its centralized counterparts.

III. Stafi Protocol

Stafi is a decentralized protocol that empowers liquidity. It encompasses 3 layers—bottom, contract and application layers. The bottom layer is mainly based on a blockchain system established by Substrate (which is a blockchain architecture developed by Parity, and the whole architecture integrates many development modules, including consensus module, P2P module, Staking module, etc.). The contract layer support creating a variety of Staking contracts, such as Staking contracts for XTZ, Atom and Dot respectively. The token holder can Stake through Staking Contract, which is consistent with the inflation incentives obtained by the ordinary Stake. But the difference is that The holder also can obtain rTokens. Last, the application layer supports third-party Stafi-based APIs or customized APIs to create a decentralized bondeds asset trading market for rTokens to circulate, transfer, and trade on the Stafi protocol.

The protocol runs in a purely decentralized manner. Stafi, which is built on Substrate, will be connected to Polkadot as a parallel chain, sharing the underlying consensus of Polkadot. The main security and performance are also guaranteed by Polkadot. The core layer is the contract level, and the ownership of the Stake token is fully guaranteed by the contract code. Stafi uses

a distributed key storage protocol to ensure the security of the Stake address through multi-signatures. The holder can initiate Stake or redeem the Stake anytime and anywhere without the need for third party intervention. When the holder of the coin initiates the Stake token to the Stake contract, the system's inflation incentives can be obtained regularly. Meanwhile, any holder of rTokens can initiate a redemption to the corresponding Stake contract anytime, anywhere (The redemption operation interacts with the original chain through the Stafi protocol. After the redeeming transaction is written to the chain, Stake coins will be sent to the submitted coin account after unlocked.) The Stafi protocol guarantees that each and every alternative rToken is exclusively correspond to the token on the original chain. That is to say, only the holder of the rTokens can initiate the redemption of the original token to the Stake contract. When A trades rTokens to B, A no longer has the redemption right to those tokens, and B now can initiate redemption to the Staking contract. The whole process does not require third party intervention.

Any third party can establish a decentralized bonded assets exchange using the Stafi protocol to at the application layer. All rToken exchanges share the depth of the transaction. With the increasing number of public chains adopting PoS launching their mainnets, the number and variety of Stake's tokens will rocket. And rTokens will traded more frequently. As a result, developers will be hugely rewarded, in the form of transaction fee, from rToken transactions they initiated.

IV. Implementation

1. Staking Contract

The contract that creates the interaction with the Stake original chain at the Stafi contract level is called Staking Contract (referred to as SC). For example, to create a XTZ-SC for connecting Tezos with Stafi. When user A holding XTZ initiates a Stake operation on XTZ-SC, the Staking Contract will first create a multi-signature address, and he will transfer XTZ through the Tezos original chain to that address.When the transfer succeeds, the contract will execute the Staking operation of the multi-sign address. If succeed, the tokens will be locked to the original chain. Then, the Stafi protocol will receive a proof of the Tezos original chain (Proofs), and then trigger the contract to generate rXTZs of equal quantities to XTZ and send them to the staker.

The update of the Staking Contract requires the original chain and the Stafi protocol to work together, for the contract status of each chain needs to be monitored, the implementation of the Staking contract shares many similarities with the cross-chain mechanism. When the holder initiates a Staking request at the Staking Contract, the generation of the multi-sign account occurs on the Stafi protocol. At the same time, the transfer of the personal asset to the multi-sign address is completed by the Stake user'_s signature. This transfer occurs on the original chain. When the Contract captures the transfer information, a Stake request is initiated from the multi-sign address to the original chain. After the Staking is completed on the original chain, Stafi captures the Stake state of the address on the original chain and verifies it,and the corresponding rTokens are issued on the Stafi protocol immediately after the validation succeeds. Throughout the process, the Stafi protocol interacts with the original chain multiple times. The monitoring and capturing of the state plays an important role in the security of the entire protocol. The Stafi protocol captures the original state by time delay and multi-pass validation to ensure the final authenticity of the original chain. Fortunately, better

than pre-existing inter-chain protocols and PoW consensus, most PoS projects launched after later 2015 see the final authenticity of block transactions as a demand that must be met. That is, when the latest height is formed, the transactions included are deterministic. At present, the common solution for the final authenticity or timely deterministic implementation is to verify the legality of the transaction before packaging the transaction to a new height. This implementation relies on the Byzantine fault-tolerant(BFT) algorithm and some artificially specified fork penalty mechanism, Slash. In view of this, the Stafi protocol has greatly improved security when interacting with the original PoS consensus chain.

2. Multi-signature Adresses

At present, almost all Stake models rely on the Account model—when the user initiates Staking, they need a private key of the original chain address to sign. In order to ensure the exclusive correspondence between the ownership of the Stake asset and rTokens, Stafi designed an intermediate address model. The ownership of assets in that address does not belong to anyone, meaning that no one can own the private key of this address. Stafi guarantees asset neutrality of intermediate addresses through secure multi-party computing technology and threshold multi-signing technology, ensuring that signatures are only performed when the holder of rTokens initiates a redemption. Secure multi-party computing involves privacy, which requires a group of certifiers with special functions in Stafi to participate. A certain number of validators, who are called Stafi Special Validator (SSV) are signed by their own private keys and transmitted through a secure channel to verify the validity of the signature, and, finally, realize the restoration of intermediate address signature. This intermediate address does not have a private key, nor is stored on the Stafi protocol. It is formed by the signature of the private certificate of the special authenticator only when the signature is required. The implementation of threshold multi-signing technology realizes that part, not all, of generators can generate the private key signature, which can greatly satisfy the need for the signature. For example, a multi-sign address establishes contact through a public key of multiple validators (say 21). When a person holding rTokens needs to initiate a redemption, only 16 signatures of 21 verifying servers are required to verify Staking and Unstake for Stake Assets.

3. Secure Multi-Party Computation

Secure multi-party computation mainly focuses on how to safely calculate a predefined function without the existence of untrusted third parties, addressing a problematic reality that a result reliant on multi-party data calculation where those parties are not willing to share the original data. With secure multi-party computation, the final result can be verified without revealing the initial input value to another third party. In Stafi's Staking contract, the user who stakes must generate a new multi-signal address. When the holder of the rToken initiates a redemption to the Stake Contract, the multi-signature address needs to create a private key signature with the involvement of special validators during calculation and generation. The validators transmit the calculation results through the encrypted channel, and they can mutually verify the results without the need to reveal their own private key. It is secured way of unlocking and redeeming the Staking Contract.

4. Ownership Transfer

When the Staking operation is completed, the redemption right of XTZ on the multi-sign address is in the hands of the holder of rXTZ. Only the holder of rXTZ has the right to redeem the XTZ-SC, other holders entitled no redemption rights. If user A traded XTZ to user B, then user A loses the redemption right to the original chain XTZ, and the mapping relationship between the XTZ and the user A address of the multi-signed address in the contract is also given to that with B. User B can initiate redemption according to his or her own wishes, or trade rTokens to other people. In this process, the multi-sign address completes multiple rounds of ownership of the original chain XTZ through the signature of special validators on Stafi who are different to that in Polkadot world—it does not requires block-producing consensus. The requirements come in only when generating the address and the changes of ownership.When user A trades the rTokens to user B, special validators (SSVs) need to conduct the signature and complete the conversion of the original Stake XTZ.

5. Stafi Special Validator (SSV)

Different from Stafi Validator (SV), a SSV is the witness of the asset ownership in the Stafi Stake contract. When the eligible holder initiates redemption to the contract, the special validator will participate in the calculation and complete the transfer of the asset from the multi-sign address to the personal address by signing. When no redemption operation occurs, the special validator stores its own private key locally, waiting to be called. A special validator is composed of multiple people picked randomly. Before the multi-signature address is formed, Stafi will select N SSVs from SVs through a random algorithm. N SSVs will be chosen by Stafi randomly to perform the calculation locally and transmit the results through a secret channel. After validation, the participation rights are obtained and stored locally on the servers respectively. The entire process is automated by the system.

At the same time, each SSV will be required to run the light node of the projects supported by Stake Contract, in order to verify the original chain trading status. This program is written to the entire special validator client and the validation is performed automatically.

6. SSV Group

In order to ensure the smoothness of the redemption channel, special certifiers in Stafi perform tasks in groups with a fixed shift. During their own shift, a single certifier group completes the multi-signal address generation and storage of the secret key, and after the execution cycle is completed, replaced by another new group. This ensures the engagement of the current verifier. One term of validators lasts an Era (1 Era is about 24hours). The election for the next group is done in the previous Era. Stafi selects new SSVs from SV candidates by block-producing rate, Staking ratio, etc,. And the new SSVs will replace the old SSVs' private key with their own ones. Meanwhile, the system will destroy the relationship established with the old SSVs' private key. However, frequent turnover will affect computational efficiency. When Stafi officially lands, it will select a reasonable replacement cycle balancing safety and efficiency.

7. System of Encouragements and Penalities for Special-Validators

Due to the importance of special verifiers, Stafi has established a system of encouragements and penalties for them, stimulating positive behaviors such as calculations and storage, and punishing negative behaviors such as disconnections and non-timely replacements. Stipulated by Stafi protocol, participation in the generation of addresses, computing, and signatures will be rewarded Stafi's token--FIS incentives. On the other hand, Stafi's penalties for security issues are severe. Stafi will require all certifiers involved in computing and storage to maintain designated online time. If the certifier is frequently dropped out, it will be slashed. If the dropping time is longer than N hours, the certifier will be Jailed and will not be able to participate in any computing and storage of the special certifier group for a period of time. In addition, the system will severely punish attacks that attempt to recover private keys and steal other people's assets based on provable data on the chain.

8. Staking Mechanism for Special-Validators

Anyone holding Stafi tokens can apply to become a special certifier of Stafi. A special certifier needs to stake FIS Token. The smuggled FIS Token is proportional to the amount of Stake that can be accepted, that is, the more FISs that are staked, the greater the value of Stake asset calculation and storage. This can effectively increase the cost of joint malicious behaviors conducted by special certifiers. The FISs that are staked will be motivated by the system, and at the same time, is also the pool of funds for system punishment. Due to the speciality of Stafi system, the requirements for the special verifier are strict, and the nodes in the early days after launch will be opened gradually to engage validators.

9. Staking Contract Security

The asset security of a Staking Contract is guaranteed in many ways. First, the asset neutrality, Staking assets will be locked to the original chain, and their mapping relationship will be recorded in the Staking Contract. Multi-signature address is guaranteed by the N SSVs through the threshold multi-signal sharing technology. So the SC is not subject to any single third party control. Second, the multi-signature address uses the asset mechanism. The special verifier is selected by the Stafi random algorithm. The verifiers do not know each other, the possibility of collusion becomes small, and the asset protection will be dynamically replaced within a certain period to ensure security. . The third is punitive. When the certifier participates in the private key signature calculation and storage, it needs to stake a certain FIS to participate. In the event of an attack or illegal behavior, the staked FIS will be Slashed, the value of the stake and can be processed. The value of the assets is directly proportional. When a variety of conditions are combined, the Stafi system can effectively punish certain risk factors. Under the assumption that most people are honest, the assets of the Staking contract can guarantee certain security.

# 10. Decentralization of Staking Contract Assets

When a holder initiates Staking through the Staking Contract, all Staking assets relationship will be concentrated in one contract. Although each Staking is initiated by a single address, it will not affect the degree of decentralization, but when the Staking assets are too concentrated, they are more easily attacked. Stafi avoids the concentration of assets by establishing several Staking Contracts of the same kind for one token. The total amount of the contract will automatically increase according to the amount of Staking assets, and the new assets will enter the new Staking contract. At the same time, Stafi will establish multiple

Staking Contracts at the primary stage. The Stafi system will equally distribute the initial Stake demand evenly among these Stake contracts, which will serve as a buffer. As the demand of Stake increases, the number of contracts will gradually be increased and differentiated by variables.

At the same time, Stafi is a decentralized open protocol. The Staking Contracts developed by initial developers will be audited and open sourced for third parties, which can create their own Staking Contracts to achieve the decentralization of Staking assets.

11. Sequence Diagram

The staking process is as follows. The user interacts with the SC first, and then the SC interacts with the original chain. During the period, in order to make the user's operation simple enough, SC needs to bear the responsibility of interacting with the original chain for multiple times. It is important that SC needs to verify the success of staking before distributing rTokens to users. The following sequence diagram shows the overall process of issuing rTokens.
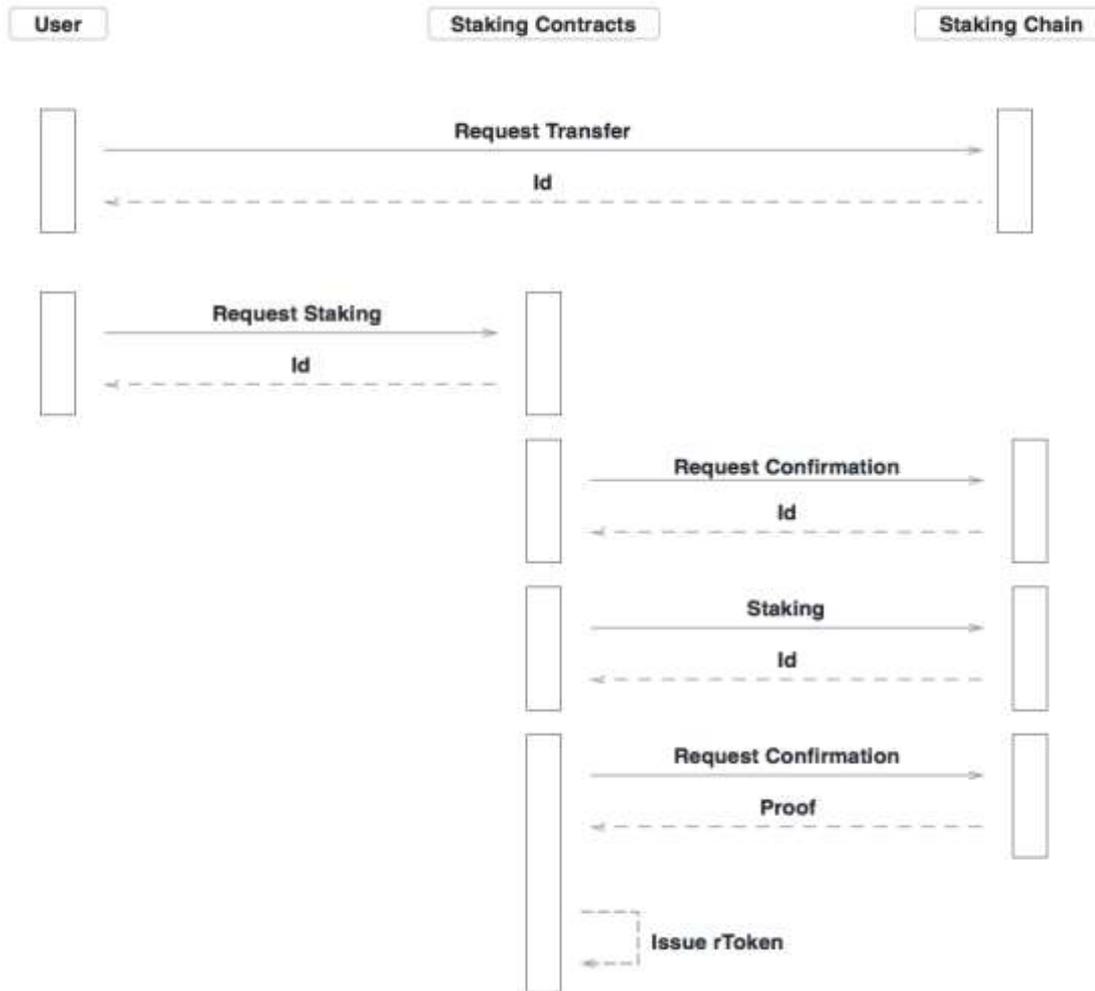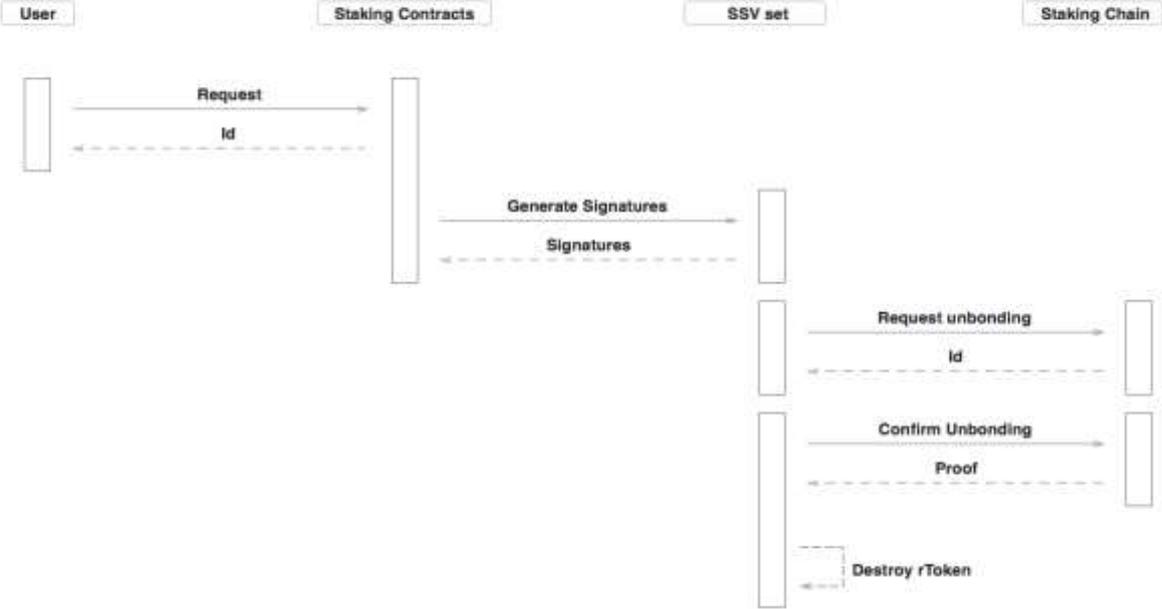
Users can redeem the assets on the original chain by rTokens they hold at any time. The modification of the relationship of the SC requires the signature of the SSV, because the record relationship of the asset is on the SC. When the user initiates the redemption, SC triggers the signature request. After SSVs execute the signature, SC interacts with the original chain and submits the Unbond/Unstake request. Then, SSV verifies the detrusting evidence on the original chain. When the evidence is true, the rTokens used to submit the request will be destroyed.

V. Upper-layer Applications

1. Circulation of Bonded Asset

The Staking contract created on Stafi releases Staking assets and can circulate on Stafi, so

users can easily trade assets to others without waiting for the original assets to be locked up. The system guarantees an exclusive correspondence between rTokens and the original chain asset, so the holder can redeem the original chain asset at any time.

In addition to being circulated on the Stafi protocol, Staking assets can also be circulated as a common asset in different blockchain trading channels, such as centralized trading exchanges. And centralized exchanges can plug in the Stafi interface and define the initial pricing of different rTokens. Because when n varies, the transaction price of each asset may change. Of course, decentralized exchanges can also list rTokens and offer a variety of matching methods. Further cooperation may lie ahead, that is the exchange can integrate the Staking contract and combine it with the users of the original chain assets on its own exchange. The issued assets are directly synchronized to the Stafi protocol. In a nutshell, when a exchange connects to Stafi protocol, it can easily complete the docking of assets and initiate transactions.

2. rToken exchange market

Stafi Protocol will provide a variety of Staking contracts for the conversion of project'_s original tokens to rTokens. Also, in order to release more liquidity, the system will evaluate different types of rTokens and establish a risk-control model. Using that model, the system can further issue FIS as the platform medium of exchange to recycle rTokens for users who want to exchange rTokens to other assets but hardly find counterparts. The exchange ratio is determined by the market and the emergency level. The further issued FIS and holding rTokens will bring extra risks to FIS holders, but the risks will be shouldered by all of them to reduce the chance of bad debts. Meanwhile, due to the price gap between rToken and FIS, when the asset is redeemed by rToken, the system will benefit from it. All are under control of that model.

3. A New Liquidity Token Protocol

Stafi Protocol, which based on SC, can provide liquidity for locked Staking assets. Meanwhile, Stafi Protocol can create more types of SCs for various Staking assets. Developers can build freely on Stafi a variety of derivatives through a set of SC development kits provided by Stafi.

4. Integration with Existing DeFi

Integration with existing DeFi mainly lies on asset level. The current Dei projects are mainly on Ethereum, and the assets are mostly Erc20 tokens. But many ERC20 tokens are relatively poor in liquidity, and the Staking Token market can be used for Defi for more liquidity and asset portfolios. Staking tokens can be achieved by bridging existing lending platforms and mortgage platforms.

VI. Tokenomics

Stafi Protocol creates value by providing liquidity of Staking assets. Staker can obtain inflation rewards while circulating rToken to respond to the market in a timely manner. The protocol captures the value of the liquidity and outputs the value to the protocol. The FIS is the native digital cryptographically-secured utility token of the Stafi protocol, FIS is a transferable representation of attributed functions specified in the protocol /code of the stafi protocol, designed to play a major role in the afunctioning of the ecosystem in the Stafi protocol, and intended to be used solely as the primary utility token on the platform.

FIS is a non-refundable functional utility token which will be used as the medium of exchange for transactions between participants of the Stafi protocol. The goal of introducing FIS is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on the Stafi protocol, and it is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt; nor is it designed or intended to be used by any person as payment for any goods or services whatsoever that are not exclusively provided by the issuer. FIS does not in any way represent any shareholding, participation, right, title, or interest in the Foundation, the Distributor, their respective affiliates, or any other company, enterprise or undertaking, nor will FIS entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. FIS may only be utilised on the Stafi protocol, and ownership of FIS carries no rights, express or implied, other than the right to use FIS as a means to enable usage of and interaction within the Stafi protocol.

Stafi protocol will create different Staking Contracts to handle different staking tokens. These staking tokens are locked on the original chain to obtain inflation rewards. When rToken is transferred or redeemed, a fee for staking rewards will be charged when the user operates. It will be proportionate to the reward, which is called Liquid Fee in the protocol.

The fees based on Staking rewards will increase with the use and the expansion of SC. The current market value of Staking Token is 1.4 billion USD, and about 60% of those tokens are locked. An optimistic estimate is that when the Stafi protocol supports the SCs of ETH2,

XTZ, ATOM, EOS, and the Staking Token unlocked by SC account for about 10% of the market, then the fees collected by Stafi's revenue will be very impressive

To calculate the fees earned by Stafi:

Earning=∑v(v∗α∗β∗γ)Earning=\sum_{v}^{} (v*α*β*γ)Earning=v∑(v∗α∗β∗γ)

Of which v is the market value of different Staking Tokens, α is the locked token ratio, β is the annual inflation rate, and γ is the circulation fee rate. We assume that the circulation fee is 30%, the average inflation reward is 5%, and the average Staking rate is 50 %.

The captured value is used to balance. The development and application of SC is an important source of income for the Stafi protocol. The inflation is to achieve the decentralization of the Stafi protocol.FIS would be distributed to provide the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on the Stafi protocol.The production of each block requires the validator to contribute their computing, bandwidth and storage resources, so the FIS generated by the same block is used to compensate the efforts made by the validator. At the same time, due to the special design of SC, protocol would also require the higher-level validators to provide security services, such as multi-signature services, light node services, oracle machine services, etc., and corresponding services will also be incentivised by the distribution of FIS tokens. FIS is an integral and indispensable part of the Stafi protocol, because without FIS, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on the Stafi protocol. Users of the Stafi protocol and/or holders of FIS which did not actively participate will not receive any FIS incentives.

All types of incentives are added together to form a one-year inflation rate. The design of the inflation rate is a complex economic problem. Through research, we find that the inflation rate of PoS projects on the market is generally set between 5 and 20% annually, most adjusted dynamically according to the overall Staking rate.

Stafi's initial annual inflation rate is divided into two parts, for the validator SV and SSV respectively. The annual inflation rate for SV is [2.5%, 10%], dynamically adjusted according to the Staking rate, and the annual inflation rate for SSV is [1%, 2%], dynamically adjusted according to the number of service calls. Theoretically, the total inflation rate will decrease year by year, and with the adoption of SC.

Token model

There are two types of tokens in the Stafi protocol, one is an alternative token (currently rToken), and one is a native token (FIS). The functions of the two tokens in the protocol are different. rToken mainly assumes the medium for liquidity, and the equity is attributed functions/right are inherited from Staking Token. As the native token of the Stafi protocol, FIS is mainly a system transaction medium, mainly responsible for value capture, consensus incentives, and prevention of system abuse (Tx fee).

1. The Staking of Validators and Incentives

An open PoS network needs to incentivize validators. At the same time, in order to prevent mischief, validators would be required to Stake FIS as a form of security deposit before participating in the validation, and after completing calculation and storage, they will be entitled to obtain the system's allocated FIS rewards. Staked FIS will be locked, and if the validator conducts mischief or wrongdoing, the locked FIS will be Slashed. The SSVs are elected from the SVs. Candidates will be assessed by several criteria, such as online time, ratio of free tokens to stake tokens, etc,. In general, for the safety of contract assets, the system stipulates that the number of Staking FIS is proportional to the number of Stake assets that can be processed, which means that the more FIS Staking, the more Stake contract assets can be processed, and you can get more FIS rewards. If the dishonest behavior of the SSVs is detected by the system, the system will also Slash on the Staking FIS, and the proportion of Slash depends on the severity of the mischief.

2. Tx Fee

The Stake Contract created on Stafi obtained the rToken circulated on the Stafi protocol through the original chain Stake. The rToken circulated on the Stafi protocol needs to pay FIS to obtain the computing power. Validators package the transaction and uploads it to the latest block data. After the latest block height is updated, rToken transactions are completed. The amount of FIS Tx fee is related to the size of the transaction data that needs to be processed. The fee model for ordinary transactions is as follows:

$$Fee_{tx}=c_{traffic}*(basefee+type(tx)*lenthOf(tx))+weight(tx))$$

Among them $c_{traffic}$ is the a parameter dynamically adjusted according to the network transaction situation, type(tx) is the parameter dynamically adjusted according to the transaction type, basefee is the basic rate, lengthOf(tx) is the data size of the transaction, and weight(tx) is a duration and status Synthesis function.

Finally, Fee is priced by FIS. If the paid FIS is higher than the resources required for system operation, the system will return the remaining FIS to the contract account after the transaction is completed. Otherwise, the system will stop running when there is no FIS payment resources.

3.Call Staking Contracts

The Stafi protocol will open multiple interfaces for third parties. Contract call will consume system computing resources. In order to limit malicious low-cost attacks and also to meet a certain degree of commercial call, when the contract call frequency reaches a certain level, the caller needs to pay certain computing resources. Of course, the business caller can customize the payer, either the platform user or the platform itself. The overall Fee model is priced in FIS. The system will calculate the computing resources and storage resources paid by the node when calling, compare the FIS paid by the caller, and determine the final model.

All transaction fees obtained from the protocol will be distributed to the SV and Protocol Treasury by a certain ratio. The parameters of the ratio can be modified through online governance.

4. Protocol Treasury

In order to achieve the decentralization and sustainable development of the protocol, part of the system's transaction fee income will be sent to the protocol treasury to support subsequent development and community work. The sources of the treasury are mainly inflation incentives, circulation fees, transaction fees, Slash deposits, etc.Via a proposal system, holders of FIS would be able to vote on parameters of the platform as well as features to be developed. For the avoidance of doubt, the right to vote is restricted solely to voting on features of the Stafi protocol; the right to vote does not entitle FIS holders to vote on the operation and management of the Foundation, the Distributor or their respective affiliates, or their assets, and does not constitute any equity interest in any of the aforementioned entities.

If the FIS in the treasury is not used up within a certain period, the burning plan will be initiated. In the early days, the Protocol eagers for much participation, so the foundation will decide the use and burning of the national treasury. When the agreement is sophisticated, the use of the national treasury will be open to the community.
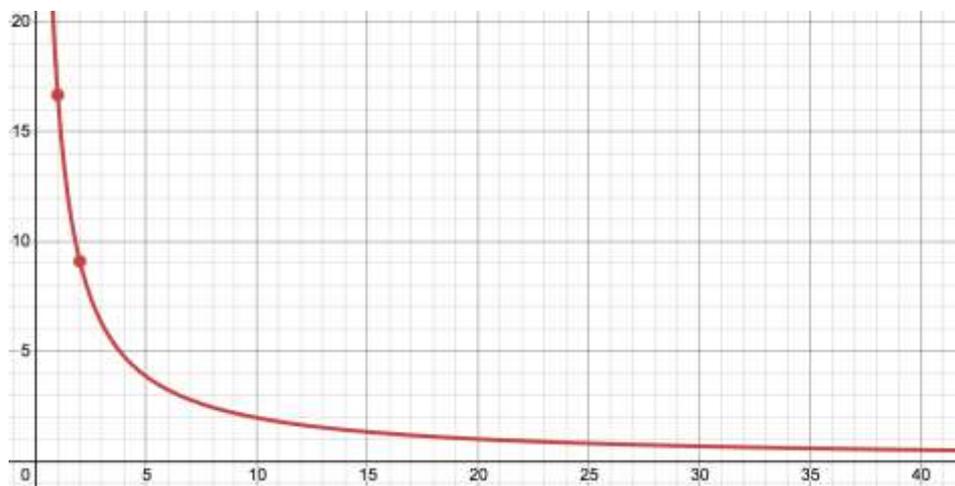
5.The Initial

Distribution of Tokens

A large part of the initial distribution of FIS is allocated to the community reward. Users can participate in staking through Staking Contracts to obtain community rewards. The amount obtained is directly proportional to the amount of work performed via total value of Staking Token. This process is called Staking Drop. Staking Drop is an initial incentive mechanisms designed by Stafi to stimulate the early adoption of Stafi. The overall value of Stafi depends on the expansion of SC. New incentives can increase the collection of circulation fees.

In order to take up a larger share of the market and attract more users, we regard Staking Drop as a long-term campaign, which will be held on an annual basis. Different airdrop periods will be tailored for different projects by their lock-up periods designated. A single project can be allowed multiple airdrops, but the scale will diminish. The initial incentive is set high enough to attract more token holders to take staking. The basic model of Staking Drop is as follows

For more about the Tokenomics of Stafi, please check Stafi Tokenomics Whitepaper.

VII. Summary

At current stage, it is must to enhance to improve the liquidity of Staking assets. With more PoS public chains launch in 2019~2020, the cryptocurrency world will welcome a sea of Staking assets. It is estimated that in the 2~3 years to come, the market value of Staking assets will reach 100 billion level, when many assets will be locked due to safety matters. The liquidity value will diminish, too. Stafi protocol starts from the Staking assets and aims at creating a decentralized alternative asset issuance protocol. At the primary stage, it will focus on providing Staking assets without the trust endorsement from a third party. Meanwhile, it will issue alternative products of Stake assets in a cross-chain manner, thus addressing the contradiction between the liquidity and safety of Staking assets. Not matter when it comes to XTZ, ATOM or DOT, DFN that will appear in the future, they will issue rTokens on Stafi protocol as an enhancement to token liquidity. Stafi provides a platform of trading and circulation for projects that demand an even higher liquidity.

For native tokens, rToken is derived from them. In the world of DeFi, however, rToken is an unparalleled underlying asset. To develop financial derivatives using rToken as a benchmark can avoid harming the security of the original chain. Therefore, Stafi will become an indispensable infrastructure for DeFi. This is also an objective in our future development.

VIII. Work in Future

There are many challenges ahead of us if we want to see rTokens circulating extensively and flourishing derivative assets based on rToken. There are challenges for technology and for trust-building also. Stafi Protocol needs protecion. The security for the Staking assets managed by Stafi Protocol is a premise. Without that, there will be no more Stakers who want Staking through Stafi. And if we have a secure Protocol, Stafi can also survive cybersecurity attacks and black swan events even if it manages a myriad of Staking assets. And with security in place, developers may willing to develop more applications based on rTokens and derive more assets.

Therefore, for Stafi, there are many work that need to be done.

- On-chain Governance

Stafi is a decentralized protocol, and its upgrade direction is closely related to governance. For many PoS consensus projects, one of the most important government approach is to set Token Staking as a voting method. The implementation may vary by different projects adopting different Staking approaches, such as stimulating the participation of voting through incentives, or providing a reference for voting by predicting the market, or even avoiding the convergence of voting result by delegation system. Stafi believes that there are a lot of voting problems in reality. Participation and voting results are widely criticized. Providing more reference and incentives can effectively solve the voting problem. However, a perfect solution does not exist in current voting mechanisms. Most of the solutions are indirect, combined with blockchain optimization. This leads to new problems. Therefore, voting is alway a tricky issue. Although the combination of blockchain boosts efficiency, but this has not addressed some fundamental issues. Stafi will implement basic voting logic in the initial stage, then

upgrade to on-chain governance logic, and put the solution of the voting problem in the long-term optimization plan.

- Private-key Maintenance Methods

At present, the private key signature of the multi-signature address is through the threshold multi-signing algorithm with the participation of multiple special validators. The validator's private key is stored on the certifier's local server (after encryption), but the asset custody and validator's existence is not permanent, so the two parties may not always reach an agreement in reality, which will endanger the storage security of assets. At present, Stafi guarantees the randomness and timeliness of private key storage through regular rotation, but frequent replacement of validators is a waste of computing resources, so the frequency needs to maintain a reasonable level. At present, the best frequency is not determined, and part of the future work will focus on striking a balance between frequency and safety.

Similarly, threshold multi-signing technology still requires trust in random verifiers. Stafi is researching new algorithms that can be used to reduce trust in order to promote protocol security upgrades. At present, the research direction of privacy computing such as MPC, TEE, etc. has potential cooperative opportunities with the security model required on Stafi. The privacy computing technology is also developing rapidly. The projects of engineered application have sprung out. Therefore, we will keep exploring in this way in the future work of the contract layer.

- Distributed Smart Contracts

When the holder initiates Staking through Stake contract, their tokens will be locked by the original chain. The security mechanism of the original chain guarantees the security of the token staked. However, due to the existence of the cross-chain bonded assets, rTokens, the mapping relationship of the asset multi-sign account will be saved in the Staking contract. When more tokens on the original chain are staked, the contract is more likely to be attacked. Although the mapping relationship is not a decisive factor in the redemption of the original chain assets, the attack would jeopardize the system. Stafi attempts to create a distribution system that will generate the Staking contract based on the value of the Staking asset. A threshold value will be set for each Staking contract. The Staking from this contract will stop when the threshold is exceeded, a new contract, instead, will be created. Dynamic setting solves the problem of asset centralization and reduces the risk of large assets being attacked.

There are sophisticated settings in the industry which can guarantee that Staking contract does not fully own locked Staking assets. Instead, when the Staking contract is called, an independent contract with only holders right will be created. The contract has a strong correlation with a single Staker. In addition, this contract will be audited by a third-party audit agency before the release.

- The Safety of Assets on the Original Chain

The issuance of rTokens relies on the proof from the original chain—rTokens will be minted and sent to the corresponding users when the Staking is done on the original chain. The Stafi protocol guarantees an exclusive correspondence between the rTokens and assets on the original chain, therefore ensuring the redemption. But if there is a problem with the Staking module on the original chain, rToken's value will depreciate accordingly. For example, if a

user stakes 10 XTZs, 10 rXTZs will be given to him. When the XTZ is made to the value of 5 XTZs because of the slash, the rXTZs will reduce correspondingly. As a result, rXTZ and XTZ will be unpegged. In order to prevent it, Stafi has designed risk control and compensation mechanism, which is described in detail in the third article of the Staking Contract series, "Risk Control Framework for Staking Contract".

This mechanism is still being polished and perfected, which is one of Stafi's future priorities.

- Distribution of Alternative Tokens

The rTokens issued through Stafi represents various rights of original staking Token (for example redemption rights, income rights, voting rights or other ecosystem rights). Staking Contracts currently realizes the basic redemption right and income right. And is developing and researching on rights and interests of rToken corresponding to the original chain, or even provide more rights and interests on other chains.

At the same time, the fairness of the distribution of rights needs to be further polished. Due to the inconsistency of the distribution rights mechanism of different PoS public chains, it will take time to perfect the SC access. The perfect products can remain exactly the same as the original chain, or even better. It is very important to establish a universal rights distribution mechanism, which can not only reduce the difficulty of development, but also improve user satisfaction. At present, Stafi adopts a simple and easy-to-understand rights and interests distribution method, adhering to the principle of the public to bear/share risk rights and interests, and distributes rights and interests to Staker. However, due to the inconsistency with the original chain mechanism, it may cause some doubts. We are still facing many challenges.

- Issuing More Alternative Tokens besides Staking Assets

The essence of Stafi is to issue alternative tokens based on Staking assets. Conversely, the basic asset for issuing alternative tokens is Staking assets. What if the underlying assets can be expanded to more forms of encrypted assets, or even derived from non-encrypted assets? If it can be achieved, Stafi's prospects will be huge. This is a medium-/long-term direction worth exploring.

References

https://multicoin.capital/2018/02/13/new-models-utility-tokens/

https://www.tezcn.com/wp-content/uploads/2018/03/white_paper_zh.pdf

https://herdius.com/whitepaper/Herdius_Technical_Paper.pdf

https://wanchain.org/files/Wanchain-Whitepaper-CH-version.pdf

Notes:

(1) The author divides the development of the PoS consensus into two stages. The first stage is 2011~2015 with the advent of the first generation PoS consensus such as Peercoin and Nxt. The second stage is 2016~present. The second generation PoS consensus was developed on

the basis of the first generation PoS consensus, such as Tezos, Cardano, Cosmos, Polkadot, etc.

(2) Staker needs to carry out Staking to participate in the PoS network consensus. In this process, the tokens participating in Staking will be locked into the system and cannot be circulated/transacted. The holder cannot respond to market changes in a timely manner. Chances of gaining a profit may be lost.

(3) The PoS consensus has computational complexity. If the weight of the Staking representative is dynamically changed during the election, the calculation will become complicated and the consensus performance will be reduced. Therefore, the Staking weight will be time-locked in a short period. It is a result taking into consideration many aspects such as performance, safety and so forth.

NOTICE AND DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER STAFI TECHNOLOGY LTD (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS (THE STAFI TEAM) WHO HAVE WORKED ON THE STAFI PROTOCOL (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE STAFI PROTOCOL IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF FIS TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://WWW.STAFI.IO/ (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

Nature of the Whitepaper: The Whitepaper and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, the Distributor, their respective affiliates and/or the Stafi team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Foundation nor the Distributor is under any obligation to update or correct this document in connection therewith.

Token Documentation: Nothing in the Whitepaper or the Website constitutes any offer by the Foundation, the Distributor or the Stafi team to sell any FIS (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or

the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of the Stafi protocol. The agreement between the Distributor (or any third party) and you, in relation to any sale, purchase, or other distribution or transfer of FIS, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Whitepaper and the Website 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 acquisition of FIS, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of FIS and/or continued holding of FIS shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of FIS (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions Documentation must be read together with the Whitepaper. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

Deemed Representations and Warranties: By accessing the Whitepaper or the Website (or any part thereof), you shall be deemed to represent and warrant to the Foundation, the Distributor, their respective affiliates, and the Stafi team as follows:

(a) in any decision to purchase any FIS, you have shall not rely on any statement set out in the Whitepaper or the Website;

(b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that FIS may have no value, there is no guarantee or representation of value or liquidity for FIS, and FIS is not an investment product including for any speculative investment;

(d) none of the Foundation, the Distributor, their respective affiliates, and/or the Stafi team members shall be responsible for or liable for the value of FIS, the transferability and/or liquidity of FIS and/or the availability of any market for FIS through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to purchase any FIS if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of FIS would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, New Zealand, People's Republic of China (but not including the special administrative regions of Hong Kong and Macau, and the territory of Taiwan), Thailand, and the Socialist Republic of Vietnam); and to this effect you agree to provide all such identify verification document when requested in order for the relevant checks to be carried out.

The Foundation, the Distributor and the Stafi team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or

reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation or the Distributor). To the maximum extent permitted by law, the Foundation, the Distributor, their respective affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of FIS should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the FIS token sale, the Foundation, the Distributor and the Stafi team.

Token features: It is highlighted that FIS:

(a) does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value);

(b) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any of their respective affiliates;

(c) does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of their respective affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the Stafi protocol, the Foundation, the Distributor and/or their service providers;

(d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(e) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment;

(f) is not a loan to the Foundation, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of their respective affiliates, and there is no expectation of profit; and

(g) does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of their respective affiliates.

The contributions in the token sale will be held by the Distributor (or their respective affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale.

To the extent a secondary market or exchange for trading FIS does develop, it would be run and operated wholly independently of the Foundation, the Distributor, the sale of FIS and the Stafi protocol. Neither the Foundation nor the Distributor will create such secondary markets nor will either entity act as an exchange for FIS.

Informational purposes only: The information set out herein is only conceptual, and describes the future development goals for the Stafi protocol to be developed. In particular, the project roadmap in the Whitepaper is being shared in order to outline some of the plans of the Stafi team, and is provided solely for INFORMATIONAL PURPOSES and does not constitute any binding commitment. Please do not rely on this information in making purchasing decisions because ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of the Foundation, the Distributor or their respective affiliates, and is subject to change. Further, the Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

Regulatory approval: No regulatory authority has examined or approved, whether formally or informally, of any of the information set out in the Whitepaper or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

Cautionary Note on forward-looking statements: All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or the Stafi team, may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Whitepaper, and the Foundation, the Distributor as well as the Stafi team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

References to companies and platforms: The use of any company and/or platform names or trademarks herein (save for those which relate to the Foundation, the Distributor or their respective affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Whitepaper or the Website to specific companies and platforms are for illustrative purposes only.

English language: The Whitepaper and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.