Swingby Connect:
A provably honest proof-of-stake based decentralized custodian

Yusaku Senga - yusaku@swingby.network

Swingby Labs

20 Aug. 2019

WORKING DRAFT

Table of Contents

Introduction

The current blockchain ecosystem has evolved so far, but it still faces two major issues: cover and cross-chain interoperability. In particular, with regard to interoperability (moving assets from one blockchain to another), there are currently various solutions that bridge the blockchain. These often require a large amount of liquidity and a large user base if the soft pegging via the self-stabilizing mechanism, the relay mechanism, the custodian solution, and the Oracle solution are self-stabilizing mechanisms. Other solutions require a specific enterprise. A custodian-based solution requires a reliable custodian. The relay mechanism (including Oracle solutions) relies on block headers created by trusted server operators.

Swingby Connect described in this document is a product for realizing a highly practical token bridge with a simpler architecture while maintaining dispersibility.

Why we need to use Bitcoin Tokens on other chains

In recent years with an increase in applications that utilize public blockchains and smart contract platforms, several blockchains and solutions still have a fundamental liquidity problem. Even with compelling decentralized applications (Dapps) and exchanges (DEX), an application or blockchain might not work well without liquidity.

Bitcoin has an overwhelming number of holders, total asset value, and above all liquidity. We believe that if we are able to make Bitcoin available and transferable to other blockchains while doing so in a trustless matter, it will enable a new surge of liquidity and opportunities.

If we could have tokens representing Bitcoin and trustless pegged to its value, a Bitcoin holder could use Dapps, DEXes, and other services without changing their main store of value to the other blockchains' native currency. native chain, such as speed, transaction fees, and anonymity, etc, whilst utilizing the underlying value of the bitcoin to which it is trustless pegged.

As a result, by realizing a “Bitcoin Token” on other blockchains, the following advantages are created:

- Bring over Bitcoin's liquidity to other blockchains
- Holders of Bitcoin will be able to use other blockchains’ advanced features and services

- Bitcoin's scalability is improved as well by offloading some Bitcoin transactions
- DEX: Blockchains like Binance Chain[1] and Ethereum[2] could provide trading of Bitcoin tokens via decentralized exchanges.

The realization of Bitcoin tokens on non-Bitcoin chains is a big paradigm shift and will help many decentralized exchanges become major. It accelerates the next generation Internet like today's Routing Protocol.

What is Decentralized Custodian.

In order to manage cryptocurrencies such as BTC and ETH, it is necessary for one entity to manage the ECDSA private key. Such services are mainly called custodians, but cryptocurrencies are different from traditional assets, and proof of asset ownership cannot connect real-world owners. Therefore, there is a risk that a single operator may not be able to set the attack target in the event of an unauthorized outflow of funds.

For businesses that guarantee the risk of such deposits, there has long been a need for a safer way to store cryptocurrency. In fact, today's trading service providers store their private keys in a secure cold wallet by multi-sig. However, such a management method hinders usability and creates the complexity of deposits and withdrawals on exchanges. That means that the risk of security incidents is extremely increased.

The safest storage method available today has long been multi-sig storage with the highest security and practicality. However, a white paper (GG18[3]) published in 2018 by Rosario Gennaro and Steven Goldfeder. Proposed the effectiveness of threshold signatures using multi-party computation.

Following this, it is now possible to construct one huge multi-sig wallet that can be joined by an unspecified number of signers.

Decentralized Custodian is a huge multi-sig wallet supported by an unspecified number of participants and is a virtual entity.

The technical core of the cryptocurrency since 2019 is the emergence of various consensus engines that have been made possible by GG18, with a distributed signature mechanism using multiparty threshold signatures. At the same time, it is expected that various services will be created to manage the cryptocurrency by an unspecified number of participants.

System Overview

The core of Swingby Connect is a multi-sig entity that can be joined by an unspecified number of people proposed by Threshold Signature Scheme (TSS) based on GG18 paper. Anyone can participate in such a multi-sig wallet, and a transaction is generated only when signatures exceeding the threshold are collected by multiple participants participating in the generation of the signature.

Swingby Connect dynamically selects the group that generates this multi-sig wallet (hereinafter TSS group) by Proof of Stake consensus and selects an unspecified number of TSS group participants.

A token bridge for one token pair has two TSS entities, and each TSS group is assigned to a one-way bridge.

System Flow: Figure. 1 below shows the system flow.

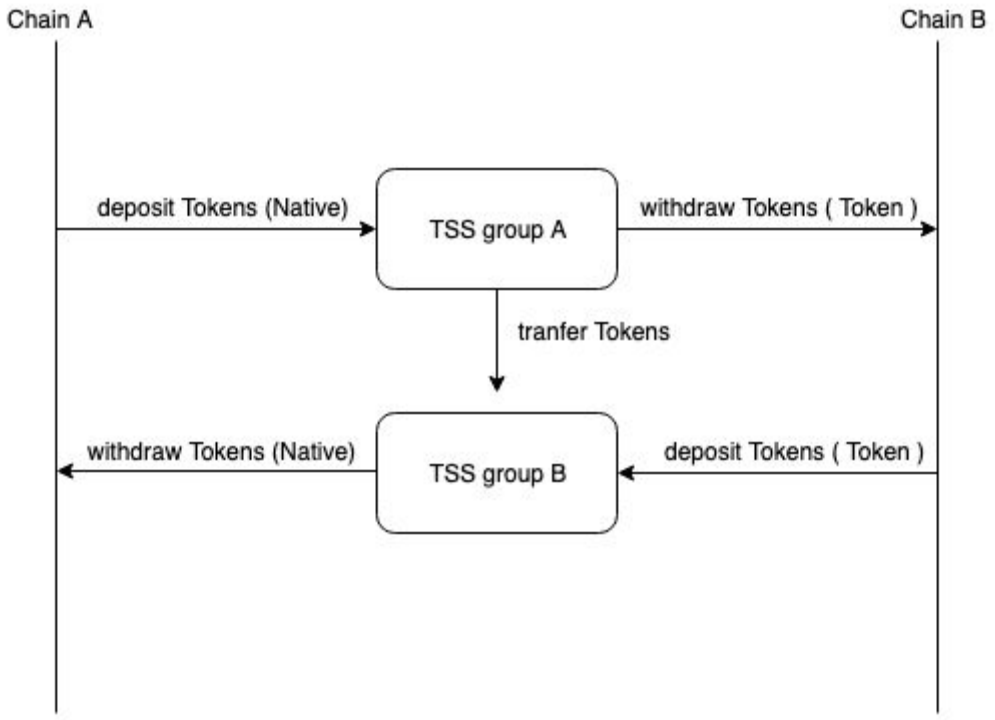

Fig. 1 System flow

The two TSS entities update participants through a Proof of Stake-based selection process. Each TSS group also synchronizes the latest state of both blockchains simultaneously to maintain the connected blockchain state. Therefore, each Node that configures each TSS group establishes a P2P session.

What is TSS

The threshold signature scheme, which is formally the (t, n) -threshold signature scheme, is multiple signature schemes. TSS is a method of creating a new multi-sig that can perform key generation using secret computation and generate a single composite signature using multiple distributed signatures. This scheme is similar to the Schnorr-signature and MuSig[4] and BLS signature[5] scheme. The BLS signature is one of the pairing signatures using an elliptic curve configuration suitable for pairing with BLS12-381. The BLS signature scheme is used as part of the Dfinity[6] consensus algorithm.

The advantage of TSS is that it differs from traditional multi-sig-like script implementations in Bitcoin because TSS multi-signature signatures are processed as a single transaction and do not need to perform on-chain script processing. Is also economical.

It is also effective for building scalable multi-sig on blockchains that do not natively support multi-sig wallets. This means that more multi-sig participants can create one multi-sig wallet and the cost on that chain is constant.

Design Goal

The basic concept and design concept of Swingby Connect are as follows.

- **Simplicity** - A combination of Proof of Stake and TSS to prevent simple multi-sig wallet management logic and complex dependencies.
- **UX focus** - Users do not like the complex peg token exchange process. The peg token exchange is done using an input TSS wallet and an output TSS wallet. These wallets are updated from time to time, but users simply send tokens to these wallets.
- **Decentralization** - A Proof of Stake-based TSS group allows anyone unspecified to participate in a decentralized custodian.
- **Safety** - TSS entities are secured according to token lock amount and lock time based on Proof of Stake. In order for a malicious cartel to attack the TSS group, a majority of tokens must be acquired.
- **Connectivity** - TSS group placement is very simple. Token bridges don't require complex smart contracts.

Technical Details

This chapter provides a more detailed technical information about Swingby Connect.

Proof of Stake Based TSS group

When creating Bitcoin tokens with other blockchains, protocol need to lock and delete Bitcoins as needed. This requires two TSS entities for input and output. Swingby Connect uses Proof of Stake to rank and order TSS group participants to build both TSS entities. This protocol measures a certain amount of time to stake a native token and select two TSS group participants. It also gives the right to join TSS entities to some of the top people.

The P2P nodes that make up this TSS group are called TSS nodes. Anyone can install the TSS node and it will automatically connect to the public node. Participation in TSS entities has an incentive to earn mining or commission revenue from native tokens. Therefore, the total native stakes required to configure the TSS group will increase or decrease depending on the frequency of deposit/withdrawal of tokens stored by the BTC TSS group. (As more nodes join, participation in more TSS entities increases, TSS node rewards increase, and competition intensifies.)

In this white paper uses a TSS group with up to 100 participants per TSS group. Therefore, The protocol needs a total of 200 nodes per pair. Since the number of nodes participating in a TSS employs threshold signatures, PoS consensus and incentive allocation is a solution to keep the number of nodes above a certain number of nodes.

Realization of TSS group on Binance chain

Binance chains do not support smart contracts, so they make TSS entities more tricky. It is processed as follows:

- All nodes update the fixed node list with each round. People with high stakes can preferentially participate in TSS.
- Each “round” of the protocol lasts 10 minutes.
- There are six of these per hour. Each “round” has a unique identifier round_num: floor (epoch_time_secs / (60 * 10))
- At least 72 hours SST cold wallet investment is required.
- Introduce new peers every night at 00:00 UTC and maintain a 100 peer pool

- TSS participating nodes are initially configured with up to 100 node pairs in two directions. This means that the maximum number of 2-way nodes per pair is 200 nodes.
- Approximately 0.1% of the transaction fee from the receiver is collected in the TSS pool and distributed to TSS group participants.

The TSS Node

As mentioned above, the TSS group is maintained in a P2P network with multiple TSS Nodes. The role of TSS Node is to communicate the messages necessary for TSS by holding and staking tokens. Also, by supporting P2P messages, TSS node can get the latest block state of the blockchain to which the token is bridged. It is the information that is required to actually deposit and withdraw tokens. These functions are effectively functioning as a decentralized oracle based on Proof of Stake.

TSS Node on the Swingby Trusted Cloud

By using Swingby Trusted Cloud[7] (STC), the behavior of each node can be publicly verified via Ethereum and IPFS[8]. The meaning is that the behavior of all TSS nodes can be verified from the outside, and Proof of Stake security can be further strengthened.

STCs also have the unique property of being physically isolated and the unique seed key that no one can access. This security guard area provides a basic solution to the malicious villain issue of TSS entities. In other words, no one knows the TSS group-generated secret share encrypted with the ECDSA private key generated using a seed key that no one can access (even the admin). This has the effect of preventing spoofed participation in the TSS group.

STC can maximize its effectiveness as an auxiliary service to run TSS nodes while maintaining confidentiality, integrity, and anonymity. Most nodes of TSS entities can be deployed to STC.

Attack Risks

This section describes attacks on Proof-of-Stake based TSS. Since anyone can participate in TSS, it is necessary to consider participation by malicious nodes.

Especially in TSS itself, in order to manage secret shares in a distributed manner, it is economically reasonable for attackers to impersonate other nodes or operate many nodes themselves to gain secret share majority.

It is best to use STC to prevent such attacks. The secret share that exists in the STC container can be hidden by the application design. Since this cannot be seen by the container owner, such an attack cannot be realized.

Blockchain finality consideration

Because it is an asynchronous system of lock chains, the use of the cross-chain protocol on two blockchains with different end requirements must be carefully considered. Especially when one of these blockchains hard forks.

Token Model

The token used in Swingby Connect is called "Swingby Staking Token" (or "SST"). Mainly used for Staking to participate in TSS group as Native Token. It will also be distributed for the growth of the Swingby network ecosystem.

SST is initially deployed and planned as a BEP-2 token in the Binance chain. In addition to the Binance chain, SST will be issued on other blockchains that can be connected to Swingby Connect. All SSTs present in different blockchains are 2-way-pegged.

Staking mechanism

To join a TSS group, participant of TSS group must lock the SST token for a period of time and obtain the right to join the TSS group. The first activation is activated in the Binance chain. Swingby Lab replaces SST ERC20 from BEP-2 first, and Swingby Connect leads the second and subsequent times. The functions of Staking itself are performed in the Binance chain, and SST is implemented as a BEP-2 token.

Token distribute schedule

The token allocation schedule is planned as follows.

- 18% Team allocation
- 24% Reserve
- 2.5% Advisers
- 2.5% AirDrop
- 18% Private Sale
- 35% Public Sale

The majority of reserved tokens will be used for protocol development support and Staking on Swingby Connect. The price at the private sale and the price at the public sale may not be constant.

Technical background and related work

In the past, various approaches have been proposed to realize 2-way peg between Bitcoin and other chains (shown below). However, there are many problems with the approaches so far, and currently there is not one running a trustless model.

Below we will go over the main approaches to realizing a 2-way peg. The examples range from methods to peg multiple and different blockchains, to relay methods and finally collateral backed stable coin method.

Trusted Custodian

Many blockchains, including Bitcoin, support the required features to be able to create a *multi-sig* wallet. Bridging a token is possible by using a *multi-sig* wallet controlled by a custodian or federation on two blockchains.

There is a project led by Kyber Network called WBTC[9] that uses this technique. They use a trusted custodian to realize an ERC-20 token representing Bitcoin on Ethereum.

However, with a "trusted custodian" model, the end users need to trust the custodian or federation. They are also vulnerable to phishing sites and server hacks. Also they need a "human trust of transaction signer". That means they have a risk of facing the unpredictable vulnerability of having a key custodian.

After all, the security is dependant on the particular key custodians who join the *multi-sig* wallet. Attackers can attack in places where risk is concentrated. Even if TSS is used to decentralize key management, It can not disperse the attack risk. The only way to improve on a trusted custodian model is to use both decentralized key management, and create a human-independent, physically trusted environment around the world.

Drivechain

The project called Rootstock (RSK)[10] wanted to provide the Bitcoin blockchain with additional *smart contract* functionality and therefore created a *sidechain* to the Bitcoin blockchain with their own implementation of *smart contracts*. In order for this to work, they require a 2-way peg method between the *sidechain* and the Bitcoin blockchain, which they proposed with a concept called "Drivechain".

Drivechain[11] is a method that uses *merge mining* for Bitcoin and relies on Simplified Payment Verification (SPV) certification. With this method it is possible to prove the movement of tokens between two blockchains in a very efficient way.

However,

- In order to realize merge mining, the mining process of sidechain is required to have the same security equivalent to the main chain
- There is a need to trust the merkle root included in a sidechain's block
- If both chains are branched on one side, it is extremely difficult to maintain consistency between both chains
- In order to realize Drivechain, a Bitcoin soft fork is required in the future

Cosmos and Peg-zones

Cosmos[12] has a concept of creating zones with blockchains and provides interoperability between them through their Inter-Blockchain Communication (IBC) protocol. However, the IBC protocol requires “fast finality” for the connecting blockchains; those blockchains therefore need a consensus algorithm that can provide this.

In order to be able to connect blockchains that do not have a “fast finality” Cosmos defines a concept of a Peg-zone which can provide pseudo finality for the underlying blockchain. The Peggy[13] is an implementation of this by the Cosmos team to provide a Peg-zone compatible with the Ethereum Virtual Machine (EVM).

Polkadot and Parachains

Polkadot[14] has a concept of a “parachain” which is any blockchain that is connected to their relay chain. Their *parachain* concept supports interoperability by using bonded validators who can move transactions from one *parachain* to another and have a slashable security deposit.

However, as mentioned in their white paper, when it comes to blockchains like Bitcoin it is more difficult because of its limited scripting capabilities. Where as with Ethereum it’s easier to achieve a secure validator rotation mechanism, with Bitcoin, providing full security for the transactions to be moved is a much bigger challenge. Currently there are no concrete plans to realize a Bitcoin bridge via Polkadot.

BTC Relay and Relay Network, Dogethereum

The BTC Relay[15] model uses SPV proofs to verify transactions from the Bitcoin network directly on the EVM.

The Relay Network is an implementation of BTC Relay that aims to minimize the processing costs as much as possible by offloading as much as possible off-chain. However, because of this the *relayer* will need to trust the merkle root that is provided, which means that you must maintain consensus among the nodes.

Dogethereum[16] realizes a 2-way peg which generates an ERC-20 token for Dogecoin on the Ethereum network. Dogethereum's 2-way peg is aiming for a decentralized storage solution for dogecoin. However, currently the Dogecoin is stored in a *multi-sig* wallet.

Collateral backed stablecoin (DAI)

"DAI"[17] utilizes a method where the value of the currency (e.g. USD) to be pegged is collateralized by another token as a collateralized bond. When the value of the token that collaterizes the currency falls or rises, the collateralized bond needs to be resolved to prevent under-collateralization. This dynamic structure of stabilizing the value of the currency represented is also referred to as a soft peg (not a perfect peg).

DAI's independent nature through decentralization of custody on the collateral is an interesting approach. When reviewing the period that DAI has been live on the mainnet until now, it has proven to be a valid technique for stabilizing the value of the token that you want to peg.

TEE and Intel SGX enclave

A Trusted Execution Environments (or "TEE") is mainly security layer technology. Representative ones are Intel SGX and ARM-TrustZone.

TEEs can remotely attest computing processes to other nodes and verify the processing state of different chips on a distance. However, current Intel chips will use an attestation service managed by intel and are known to be vulnerable to side channel attacks. It is easier to reproduce a secure execution environment but for the current options on the market it can not be used as a decentralized tool.

Road map

In the initial release, Swingby Connect and SST will be released on the test network by the end of the third quarter (alpha test).

The second release supports the generation of Swingby Connect BTC tokens on the Binance chain and the exchange of SST tokens on the Binance chain test net. Including TSS UI development by the end of Q4

After the second released, we plan to release the main net through security audits, stress tests, and emergency response tests for the main net release

References

[1] Binance, Binance Chain (DEX)
https://docs.binance.org, 2019

[2] Vitalik Buterin. Ethereum - A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM
http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Rosario Gennaro, Steven Goldfeder. Fast Multiparty Threshold ECDSA with Fast Trustless Setup (GG18)

[4] Gregory Maxwell and Andrew Poelstra and Yannick Seurin and Pieter Wuille, Simple Schnorr Multi-Signatures with Applications to Bitcoin
https://eprint.iacr.org/2018/068, Jan 2018

[5] S. Mitsunari. Barreto-Naehrig curve implementation and BLS.
https://github.com/dfinity/bn, 2017.

[6] Timo Hanke, Mahnush Movahedi and Dominic Williams. DFINITY Technology Overview Series Consensus System
https://dfinity.org/static/dfinity-consensus-0325c35128c72b42df7dd30c22c41208.pdf

[7] S. Yusaku, Singby Trusted Cloud
https:/stc.swingby.network

[8] Juan Benet, IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[9] Kyber Network, BitGo Inc, Republic Protocol. Wrapped Tokens - A multi-institutional framework for tokenizing any asset.
https://www.wbtc.network/assets/wrapped-tokens-whitepaper.pdf, Oct 2018

[10] Sergio Demian Lerner. RSK White paper Overview.
https://docs.rsk.co/RSK_White_Paper-Overview.pdf, Nov 2015

[11] Drivechain - The Simple Two Way Peg http://www.truthcoin.info/blog/drivechain, Nov 2015

[12] Jae Kwon, Ethan Buchman. Cosmos - A Network of Distributed Ledgers
https://cosmos.network/cosmos-whitepaper.pdf

[13] Cosmos. Peggy https://github.com/cosmos/peggy

[14] Gavin Wood. Polkadot: Vision for a Heterogeneous Multi-Chain Framework
https://polkadot.network/PolkaDotPaper.pdf

[15] BTC Relay https://github.com/ethereum/btcrelay

[16] Dogethereum Contracts https://github.com/dogethereum/dogethereum-contracts

[17] Maker Team. The Dai Stablecoin System.
https://makerdao.com/whitepaper/DaiDec17WP.pdf, Dec 2017