BSPC

A multi-institutional framework for tokenizing any asset

Bitstamp Pro

Whitepaper v0.2
July 24th 2021

Abstract

BSPC token is the trc-20 native functional token of Bitstamp Pro platform.Defi Mining: BSPC holders can get a unique NFT on Bitstamp Pro bank.Defi lending: holding BSPC mining on the chain, participating in non-destructive lending on the chain, helping non-destructive mining to improve computing power

Bitstamp Pro

- Bitstamp Pro- This is a mechanism followed by some tokens on Bitstamp Pro-where demand and supply are controlled by smart contracts in order to keep the price of the token in line with a fiat currency. Some examples of this are Dai, Basis, Carbon, and NuBits

- Bitstamp Pro- Assets are stored with an organization which publishes proof of reserves. This is the case with Tether, True USD, USDC (USD), Digix (gold), Globcoin (a mix of fiat

Mission and exclusive NFT delivery.NFT and Governance: BSPC holders can vote on platform parameters, including partial ownership of NFTAnd participate in the decision-making of community space.NFT creation: creators lock BSPC into the market and promote its cultural collections.

Bitstamp Pro: around NFT + defi, Bitstamp Pro will build a set of defi liquidity mining; NFT assets, transactions, financial chain bank intelligent contract system. It also provides users with one-stop NFT asset management, trading, auction and Finance (mortgage, lease, composition and splitting).

Wrapped tokens follow the centralized model, but instead of relying entirely on one institution, they rely on a consortium of institutions performing different roles in the network. This whitepaper proposes a framework for issuing asset backed tokens by addressing challenges with scalability, trust, regulation, and governance. The first wrapped token we launch will be an ERC20 token backed by TRX and will be appropriately named, “BSPC" (BSPC). Unlike centralized solutions (USD), WBTC will be fully accounted for and proof of reserves posted on the TRX chain.

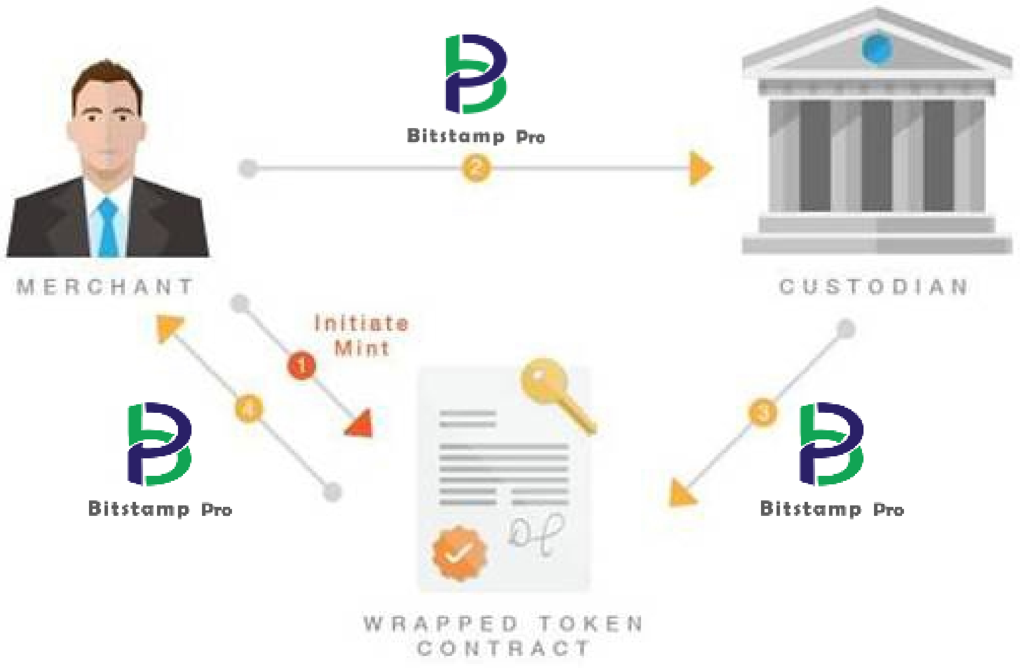
There is no additional secondary utility/payment token required to use BSPC, and no transfer fees other than blockchain fees. BSPC uses a simple federated governance model and strives to promote usability.

BSPC

The total issued amount is 66 million, 10% of which is from the foundation. At the beginning of May every year, 10% of the money is released, 5% is from community construction, 85% is used for community autonomy and voting construction, and 56.1 million yuan is used for mining in 12 years

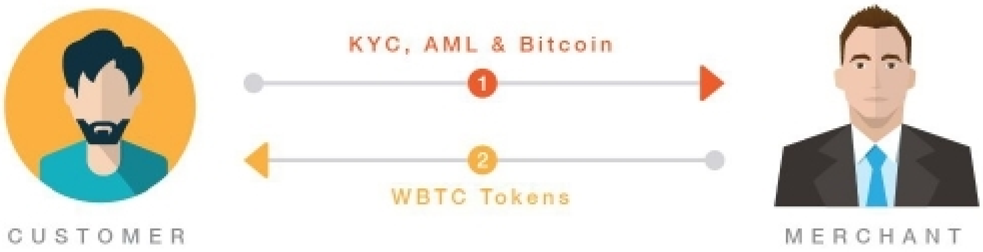
Reduce production by 50% every three years (29.92 million RMB in the first stage, 14.96 million RMB in the second stage, 7.48 million RMB in the third stage and 3.74 million RMB in the fourth stage) and deflate to 21 million RMB

Participating in Mining: usdt (TRX real-time equivalent usdt) participates in mining, usdt: BSPC proportion is 7:3 mining, and the profit is doubled. BSPC participates in mining, and the profit is doubled. The electronic card can be drawn once a day, and the corresponding electronic card can be collected to obtain the profit machine, which can be used to borrow money from BSPC



Sequence of minting events for MBP

- Merchant initiates a transaction to authorize the custodian to mint X WBTC to the merchant's address on the Ethereum chain.
- The merchant sends the custodian X BTC.
- Custodian waits for 6 confirmations of the BTC transaction
- Custodian creates a transaction to mint X new WBTC tokens on the Ethereum chain

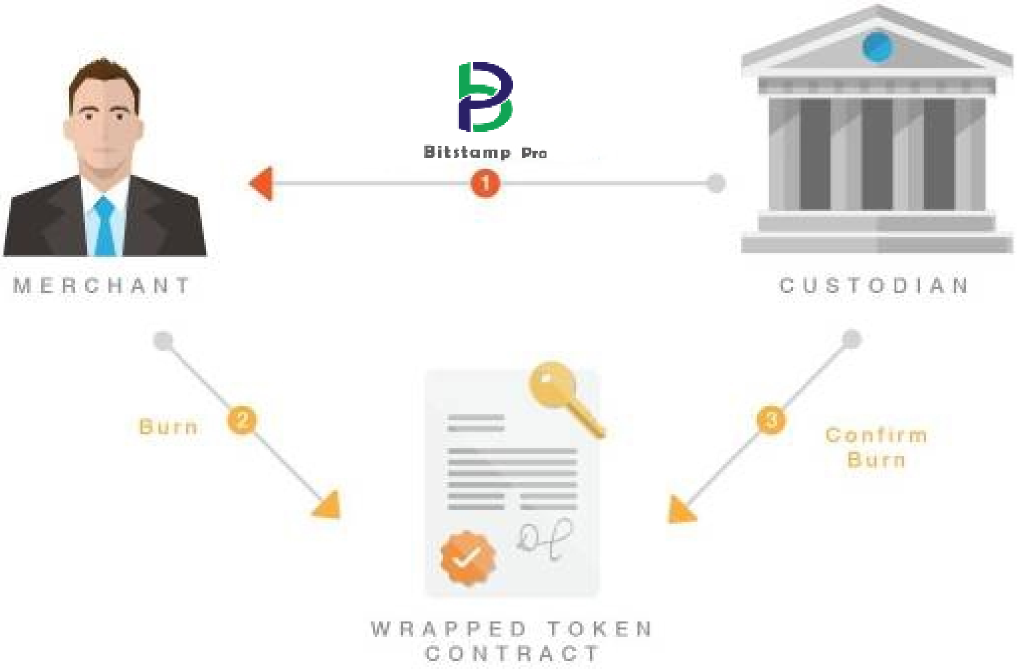


Sequence of events for users to receive BSPC tokens

- User requests wrapped tokens from a merchant
- The merchant does the required AML, KYC procedures and gets identification information from the user
- The user and merchant perform an

Burning

Burning refers to the action of redeeming BTC for BSPC tokens. Only merchant addresses can burn wrapped tokens. In order to do so, the 'burn' function is called in the contract with the amount of tokens to be burnt on the Ethereum chain. By doing so, the amount is deducted from the merchant's BSPC balance (on chain) and the supply of WBTC is reduced.



`

Sequence of events for burning BSPC tokens

- The merchant creates a burn transaction, burning X BSPC tokens
- Custodian waits for 25 block confirmations of the ETH transaction
- Custodian releases X BTC to the merchants Bitcoin address
- Custodian makes an ethereum transaction marking the burn request as completed

Bitstamp Pro the Bank of the Philippines, was established in March 2020 to solve mining problems for users through smart contractsThe security of funds. The smart contract is designed so that all private keys are in the hands of users, and no one can access themTake your money, your assets. Defi predictors are often centralized and rely on a third party to be reliable and timelyProvide critical information in an urgent Bitstamp Pro: aims to break this gap by providing information to smart contracts through decentralized Oracle networksThese predictions work together on the Bitstamp Pro contract to validate and forward key information to theThese Bitstamp Pro: the network allows users with data feeds or information hosting APIs to easily connect to the smart phoneAbout to provide information to mine money.

BSPC

Tokenization

The act of tokenizing assets can:

- Increase speed of transactions
  Ethereum blocks are created every ~15 seconds and it is possible to have a fair deal of confidence in the irrevocability of a transaction in less than 5 minutes. This speed is faster than transacting natively compared to many other assets including Bitcoin, gold, and fiat currencies
- Reduce the number of intermediaries
  One of the key benefits of assets on a blockchain is their ability to be transacted without intermediaries. This can be done through atomic swaps, decentralized exchange protocols, and lightning/raiden style channels.
- Enhance security
  Tokenization enables users to have full control of private keys of the asset. Users who do not want to hold keys can reduce counterparty risk by moving it from exchanges to a security-focused custodian.
- Usability
  The NFT standard has been adopted by a large number of institutions and products. This provides users with a variety of exchanges, wallets, and Dapps to use while handling their tokenized asset. They also have the ability to move tokens quickly, 24/7.
- Improve Transparency

In the first three years, a block was blasted every 45 minutes, which cost about 865 yuan, 27700 yuan per day for mining, 40% for static miners and 60% for dynamic miners. Select mining period:

15 days 85% lock up 180 days release 15% free trade 20% loan

45 days 80% lock in 180 days 20% free trade 30% loan

90 days 70% lock in 180 days 30% free trade 40% loan

cryptocurrency can replace traditional finance. Notably, it can be used in e-commerce by both buyer and seller without having to worry about conversion rates or taxes (buyers are required to pay capital gains tax calculated at the time of purchase in the US).

Interoperability between cryptocurrencies

As we see an expansion in the number of cryptocurrencies today, each one focuses on some aspect of monetary exchange. Some such aspects are transactional throughput, privacy, cheap transaction fees, smart contract ability, and decentralization of nodes/miners. The wrapped framework would make it easy to represent any other cryptocurrency, such as Bitcoin, on Ethereum and thereby enhance it with all the capabilities of the Ethereum blockchain. One such use case is the ability for initial coin offerings (ICOs) to be directly funded and mint tokens on deposits of wrapped Bitcoin tokens. In the future, centralized exchanges and other institutions which accept cryptocurrencies would not need to maintain multiple cryptocurrency nodes and instead could just develop on Ethereum.

On chain ways to enforce policies

Tokenization also provides a way to enforce policies on chain. On chain policy enforcement makes rules more transparent and doesn’t rely on one single party to enforce them. Based on the type of asset, there could be a need to enforce rules on asset transfer or trade. Securities for example require whitelisting, holding periods, and identity management.

Common Issues

combustion deflation is as follows

1. Currency price multiple growth burning 10% of the produced currency

2. 2. If the funds are less than 5000U on the same day, 10% of the coins will be destroyed on the same day,
3. 30% for two consecutive days, 50% for three consecutive days, and 10% for the fourth day

- Is the asset holder authorized in the existing legal framework to hold the asset?
- Can the custodian create an arbitrary amount of tokens?
- How does the custodian prove possession of the asset under custody?

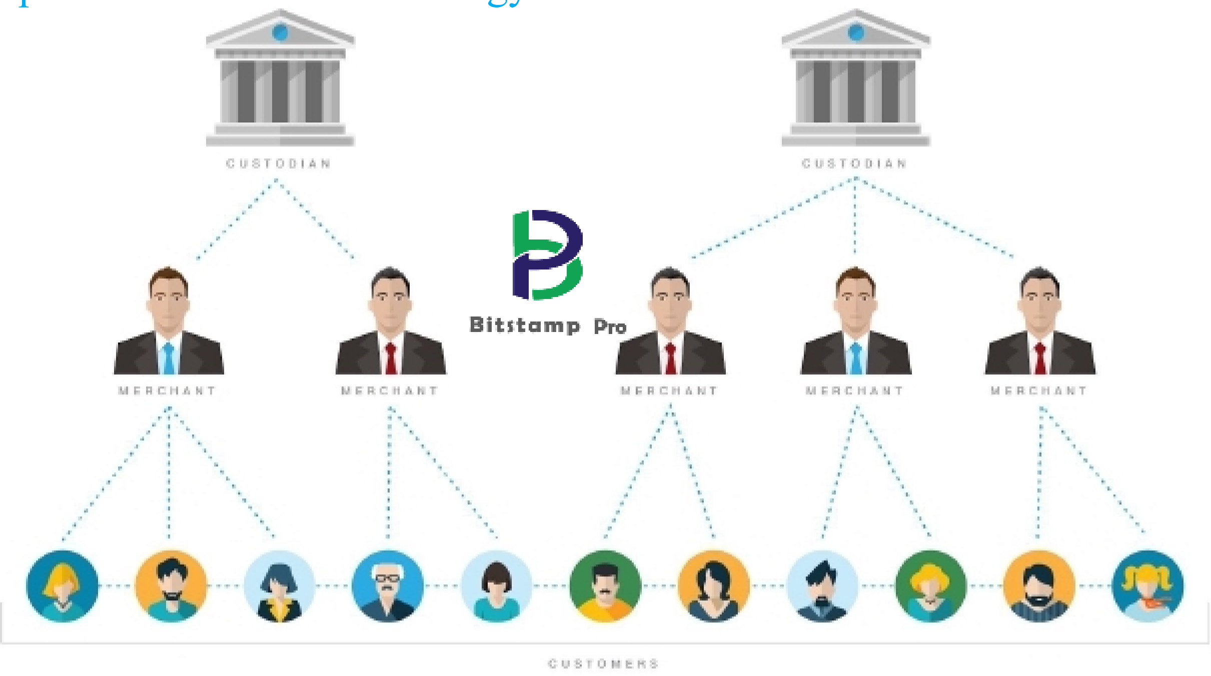
Regulation

Custodians of asset backed tokens need to be licensed to hold the asset. This license may vary based on the asset and geographical jurisdiction of the custodian. Custodians must also prove reserves regularly given that a lack of 1:1 backing would undermine the whole system. KYC and AML restrictions also apply to users engaging in asset backed tokens. These restrictions need to be enforced at the time of purchase, redemption, or transfer of tokens.

Governance

When there are multiple stakeholders in the system, there is a governance challenge with how to handle changes made to the token. Most asset backed tokens are entirely reliant on the asset custodian to make changes to the rules/smart contract governing the token. Usually in the case of ICOs, the issuer of the token has full control of protocol changes. There have been some cases like decentralized autonomous initial coin offerings (DAICOs) where users have voting rights, but they face the challenge of a low voter turnout [3].

Implementation and Technology



Key Roles

- Custodian - The institution or party who holds the asset. In the case of BSPC this will be played by BitGo
-

Boxer 36164; Boxer 22330; Foundation of Foundation Bitcoin Suisse; DMC; Greylock Partners; True Ventures; HASHKEY; Boxer 36164; Boxer 36164;

BSPC, this will be played initially by Kyber [5] and Republic Protocol [6]. Each merchant holds a key to initiate minting of new wrapped tokens and burning of wrapped tokens.

- User - The holders of the wrapped token. Users can use wrapped tokens to transfer and transact like any other ERC20 token in the Ethereum ecosystem.
- BSPC - Contract changes and addition/removal of custodians and merchants will be controlled by a multi-signature contract. Holders of the keys to the multi-sig contract will be held by institutions as part of the BSPC

Custodians exchange assets for wrapped tokens with merchants. This is done through two different types of transactions; minting (creation of wrapped tokens) and burning (reducing supply of wrapped tokens). These transactions will be available publicly and can be viewed by anyone through a block explorer. After the initial exchange, merchants aim to maintain a buffer of wrapped tokens so that they can exchange it with users. The two-step minting process helps reduce the time it takes for users to get wrapped tokens, as minting and burning are more time consuming processes.

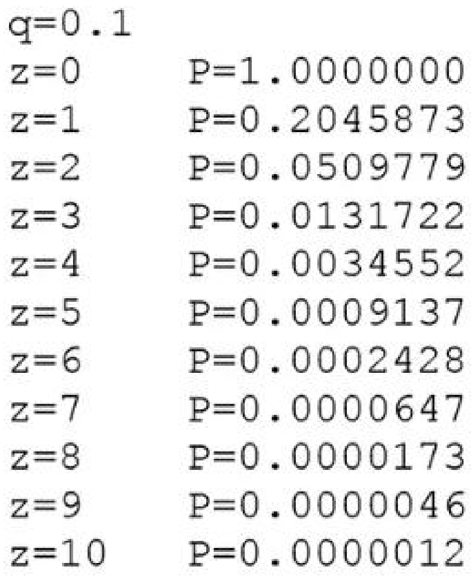
Custodian wallet setup

Custodians are expected to have a pooled wallet for all merchants. The wallet will use multi-signature with all keys controlled by the custodian. The wallet will only be able to send to the whitelisted merchant address on chain. All minting and burning transactions are expected to be done within 48 hours of submission to the custodian. Note that in case of multiple custodians, a single wallet might not have enough funds to redeem all pending wrapped tokens.

Minting

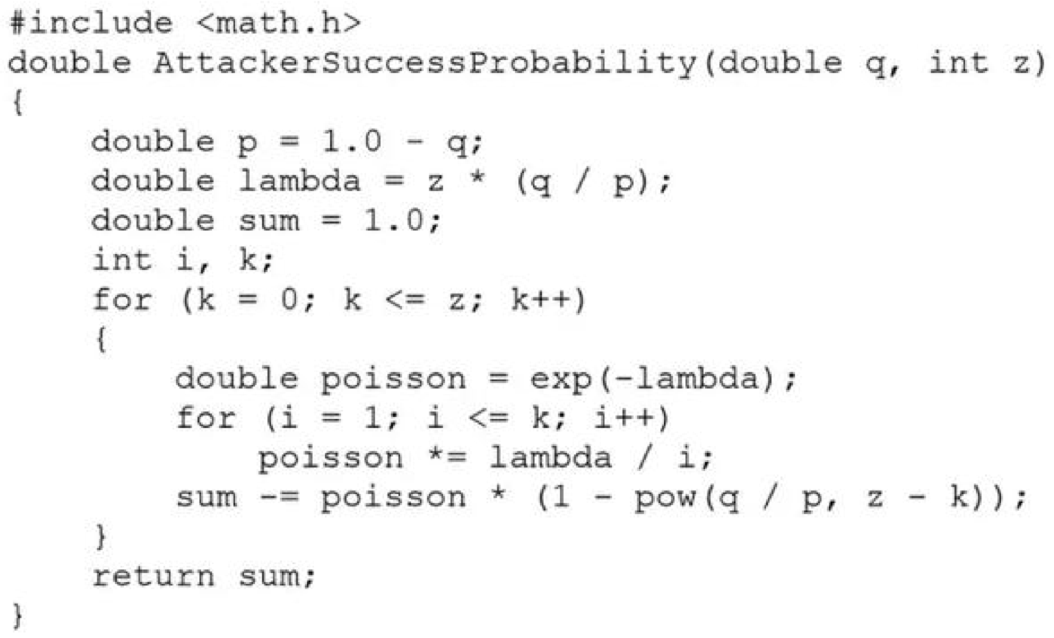
Minting refers to the process of creating new wrapped tokens. Minting in the wrapped framework has to be done by a custodian, but needs to be “initiated” by a merchant. It is important to note that minting does not involve the user. It is a set of transactions done between the merchant and the custodian.

In this case, in order to calculate the probability of the attacker catching up, we multiply the probability density of the Poisson distribution of the number of blocks that the attacker has made progress by the probability that the attacker can still catch up under this number.



```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

Although it is possible to deal with a single currency, it will be very inconvenient to separate a transaction for each currency in a single transfer. To allow value segmentation and consolidation, transactions include multiple inputs and outputs. Generally, either a single input from a previous larger transaction or multiple inputs with a smaller amoun



```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Given a hypothesis, P > Q, the probability decreases exponentially as the number of blocks the attacker has to catch up with increases. Because the odds are against it, if he is not lucky enough to make a big leap in the early days, he will be left far behind and his tampering will be negligible.

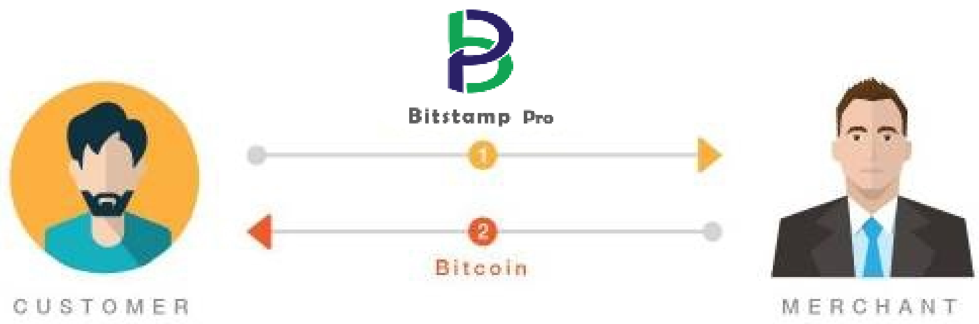
$$q_z=\left\{\begin{array}{cc} 1 & \mathit{if}\ p\leq q \\ (q/p)^z & \mathit{if}\ p>q \end{array}\right\}$$

We now consider how long the payee of the new transaction will have to wait until it is fully determined that the payer cannot modify the transaction. Let's assume that the payer is an attacker. He wants the payee to believe that he has paid at that time. After a period of time, he will pay himself instead. When it happens, it will alarm the payee, but the payer hopes it is too late

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left\{\begin{array}{cc} (q/p)^{(z-k)} & \mathit{if}\ k\leq z \\ 1 & \mathit{if}\ k>z \end{array}\right\}$$

The payee creates a pair of new keys, gives the public key to the payer, and reserves a short time before signing. This will prevent (the following things) from happening: the payer prepares the blockchain in advance by working continuously until he is very lucky enough to get far ahead (that is, his blockchain length exceeds the honest blockchain length), and then executes the transaction.

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$



Sequence of events for users to BSPC

- User requests the redemption of tokens from a merchant
- The merchant does the required AML, KYC procedures and gets identification information from user
- The user and merchant perform an

On Chain transfer restrictions

Based on the token, there could be restrictions in place for the transfer of tokens. For WBTC, there will be no restrictions on transfers.

DEFI

A real and valuable defi needs six elements:1. Open source code, which can be found on GitHub or block browser.
2. After being audited by a well-known large safety audit company, an audit report was issued,Prove that the code is safe and there are no loopholes. According to the contract, there is no rat storehouse and secret door
3. With excellent technical strength, ability and experience, we have successfully built this defi product,And will carry out later development, maintenance and upgrade4. Robust and feasible economic model5. Successful and excellent consensus mechanism6. Professional and powerful ground promotion team

NFT

NFT English full name for non functional token, Chinese called heterogeneous token, a kind of digital cryptocurrency. NFT is a kind of cryptocurrency recorded on the distributed accounts of the blockchain. The origin of NFT comes from the art collection circle. NFT gives digital works unique certainty, which is irreplaceable. It is NFT that gives digital works this certainty. Thus, it ensures the security and reliability of "certificate" and "permanence" in a certain sense. NFT can replace digital assets to trade and circulate. Trading NFT means trading the ownership of digital assets.

DeFi+NFT

The two main advantages of the defi ecosystem are mobility mining and NFT mining. The integration trend of NFT and defi under the influence of defi products in 2020, the new generation of NFT products are more and more combined with defi protocol, NFT products gradually become more complex financial documents from simple collection certificate.

The developer community turned to the combination of NFT and defi applications, and soon won the support of native users of blockchain. The reason is that the mainstream NFT products have entertainment attributes, and the later incentive mechanism has financial attributes.

This can be done through the use of a pegged sidechain, using existing software (parity-bridge) run among DAO members. The chain will run on it's own proof of authority network

- Scaling with minimal development costs (same EVM)
- Dedicated, increased throughput - seperate blockchain on separate hardware and potential proof of authority (PoA) advantages (faster blocks)
- Easy to support in existing clients and wallets
- Chain is free from other "noisy neighbors"
- Minimal transactional cost (to prevent spam)

Validators (block generators) will be chosen from wrapped partners and other trusted parties who will be geographically distributed and represent several different domiciles / governments. Validators will also maintain the 2-way peg between the main and side chain. To peg the value of wrapped tokens on both chains, we propose a multi-signature contract to be used on the mainnet and the sidechain.

- To send from Ethereum mainnet to Ethereum sidechain:
    - Send from mainnet address to the federated mainnet multi-sig address
        - It is recommended to send the amount while calling the “sendToSidechain” method on the multi-sig address, specifying as the argument the destination address on the sidechain
        - If sent without a method, the destination address on the sidechain will be assumed to be the same as the source address
    - An event is generated on the mainnet to record the send
    - Federated signers “lock” tokens on mainnet
    - After a “confirmation period”, multisig authorities on the sidechain can validate the send event on the mainnet and disburse the amount to the destination address on the sidechain, less transaction fees
- To send from ETH sidechain to ETH mainnet:
    - Identical (symmetric)

BSPC will be the first asset on the sidechain and will use a combination of these components working together to create an ecosystem:

- Node Software and Configuration
- Block Explorer
- Wallet Providers

- Block Validators
- Multi-sig Authorities

Incentivization

Transactions will be charged at the minimal starting gas price of 1 Gwei to cover running block validators and to prevent spam on the sidechain. Validators can also be incentivized off chain for each Dapp or have block rewards. Details of distribution/management of Ether on the sidechain are still to be determined.

Atomic Swap of BSPC

Atomic swaps can be used between merchants and users in order to exchange BSPC and BTC. If the user would like to receive WBTC or BTC more quickly, a trusted method of exchange could also be done through the merchants.

Once KYC is completed, the steps for users to atomically swap BTC for BSPC with the merchant are:

- User generates a secret and a hash of it is provided to the merchant off chain. The user and the merchant also agree on other swapping details such as receive addresses (TRX and TRX)
- The user creates a Bitcoin HTLC (Hashed Time Lock Contract) using the merchant's Bitcoin address, user's refund address, secret hash, and expiration time. This is used to create a P2SH address which the user funds with TRX
- After 6 confirmations, the merchant will create an HTLC contract on Ethereum, by using the user's Ethereum address, merchant's refund address, secret hash, and expiration time. The merchant then transfers X BSPCC to the atomic swap contract.
- The user reveals the secret in order to move X BSPC from the atomic swap contract to the user's Ethereum address
- The merchant uses the secret in order to move Bitcoin funds from the P2SH address
- If the user does not claim the BSPC within the expiration time, the transaction does not go through and the user can claim the BTC back

Some important things to note here:

- In order to deploy the atomic swap contract and send BSPC to it, there are transaction fees involved. Hence, the user will have to pay an atomic swap fee before initiating a swap.
- Atomic swaps take time and multiple transactions on both the BTC and TRXchain. The user may have the option of doing a trusted swap in which BTC is transferred to the merchant address and after 6 confirmations on the bitcoin network, the merchant sends WBTC to the user. This involves trust in the merchant, but it is quicker and cheaper.

BSPC

Atomic swaps can be performed without BSPC for users which only want to perform a BTC-ETH trade. They can be done on a decentralized exchange outlined through a mechanism by the Komodo platform [9]. However, it is important to note that BSPC provides a representation of TRX on the BSPC chain, which is required for DAPPs and the ecosystem to interact with. A few other tradeoffs to consider while comparing atomic swaps with BSPC:

- They require price discovery to be done by whoever does the atomic swap. In wrapped tokens price discovery only needs to be done while trading on a decentralized exchange after having already obtained BSPC.
- Requires atomic swap technology to be supported by existing wallets and decentralized exchanges. Wrapped BSPC will be available for use in any ERC20 supported wallet.
- They are really slow because every transactions is as slow as multiple confirmations on the TRX chain and then the Bitcoin chain (as opposed to BSPC, where the initial minting/tokenization is slow but after creation it's easily tradable on the TRX chain)
- Doing an atomic swap on a decentralized exchange requires a separate deposit and a

- Custodian fees: This is taken by the custodian at the time when a merchant mints or burns wrapped tokens.
- Merchant fees: This is taken by the merchant who the user exchanges wrapped tokens with for the asset.
- Sidechain transaction fees: This fee is predominantly aimed at preventing spam on the sidechain. This is shared equally among all institutions running nodes on the sidechain.

Legal Binding

Contract between custodians and merchants

The process of minting and burning tokens does not involve the user and is between trusted institutions. Merchants are required to hold the identity information of the user securely. Custodians are required to publish details of assets under custody quarterly and perform minting/burning duties in a timely manner. Failure to meet these criteria can lead to removal from the network.

It is to be noted that there can be multiple custodians in the network, but this comes at the cost of increasing the risk involved in the network. A model where custodianship is shared by different institutions holding keys to a multi-sig wallet is also possible in the future. Though operationally, minting/burning/auditing would require more coordination and time. A security breach among any of the custodians would cause the loss of trust and could lead to mass withdrawals. A security breach with a merchant is much less severe as all outstanding tokens will still be backed up by custodians, but instead could lead to a loss of KYC/AML user data.

Security

BSPC 's high security, low power consumption and rich integrated environment may provide convenience for more NFT combined with defi innovative products

- Quarterly audits will be conducted by external third parties to verify that all wrapped tokens minted have an equal amount of asset stored among all custodians. In the case Of BSPC, proof of reserves can be shown by publishing signatures from the addresses which bitcoin is stored in.
- Custodians will not be able to mint tokens on their own, but would instead require the initiation of a merchant in order to do so. Hence creation of new tokens involves both the custodian and the merchant.
- The user is insulated from interacting with the custodian through a set of merchant institutions. An individual merchant does not need to be trusted, but instead all merchants together would need to be.
- Existing credibility of the institutions involved is at stake for all the institutions involved with the framework.

Value

There will be full transparency in the functioning of the wrapped token. All key details of the network will be reflected in a dashboard, some of which are:

- Names and details of institutions performing different roles in the network
- Status of mint and burn orders (pending, processing, cancelled, complete)
- Total amount of BTC stored by custodians
- Total amount of BSPC in the network (Will be the same or slightly lower than BTC stored)
- Quarterly audits in the form of transactions which prove that the custodian has the keys to the Bitcoin
- Merchant and Custodians ethereum addresses
- The Bitcoin address associated with each merchant, controlled by the custodian
- Links to the open source token contract code / deployed contract on a block explorer

BSPC’s future

In the near future, we will see more blending between defi and NFT. As NFT products gradually walk out of the “ entertainment collection" ecology and become more and more valuable, developers' demand for security performance and efficiency also increases.

BSPC 's high security, low power consumption and rich integrated environment may provide convenience for more NFT combined with defi innovative products