DeCus LitePaper V1.0

What is DeCus?

DeCus is a high capital efficiency cross-chain custody system based on innovative algorithms. We offer a trustworthy infrastructure that allows tokens to flow across different blockchains and that provides a safe way to leverage the utilization rate of crypto assets.

WhatiseBTC?

Tokenized bitcoin is another frequently used pegged value crypto asset. The underlying assets, BTC, are kept by one party or multiple parties and then a certain party mints or issues a token on another blockchains (currently, that is the Ethereum blockchain) with the same value as regular BTC but which possesses the same functionality and use as an ERC-20 token. Some examples of tokenized bitcoins include WBTC, HBTC, tBTC, renBTC, sBTC and so forth.

eBTC is an ERC20 token backed 1:1 with real BTC. As the first usecase for DeCus, eBTC provides a better solution for tokenized bitcoin with improved efficiency and decreased risk in a truly decentralized way.

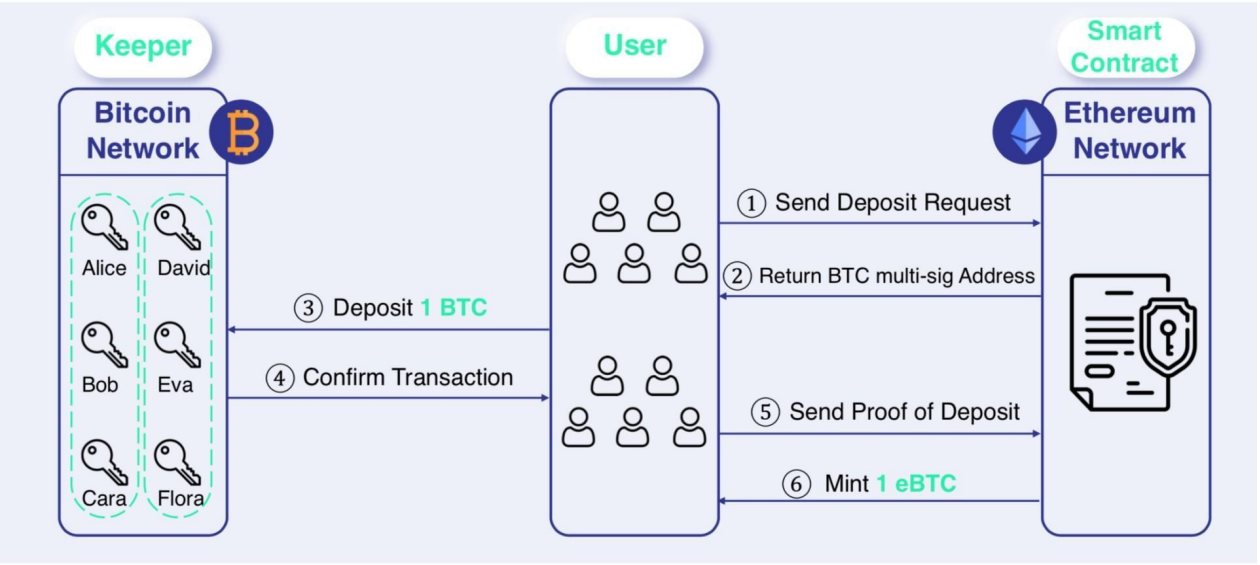
How does the systemwork?

At the core role of the whole system is the Custodian Network, which is responsible for the custody of underlying crypto assets and provides crypto collateral against system security risk.

Running nodes is another responsibility for Keepers. They must have a cloud server in order to configure private keys for the Ethereum Network to verify identities and interact with smart contracts, and to generate a pair of keys to initiate and verify Bitcoin multi-sig transactions.

Smart contracts deployed on target blockchains will mint the relevant pegged value crypto assets. The whole process is organized in a 100% decentralized way given that it is permission-less for Keepers to join or leave the Network at will. Users can cross chain their crypto assets in a secure and decentralized way up to a capacity backed by the crypto collaterals provided by the Custodian Network.

The proprietary algorithm of DeCus allows Keepers to operate as decentralized Keepers at a low collateralization rate, but with the security of custody still guaranteed, thereby improving the utilization rate of crypto assets.



DeCus will initially launch with with tokenized bitcoin-eBTC, with the process illustrated in the following chart.

A user who wishes to mint eBTC first submits a request to the smart contract on the Ethereum network and then is given a multi-sig BTC address of a designated Keepers group. Once BTC has been deposited to that multi-sig address and proof of deposit has been submitted, the corresponding amount of eBTC is sent to the user's ETH address.

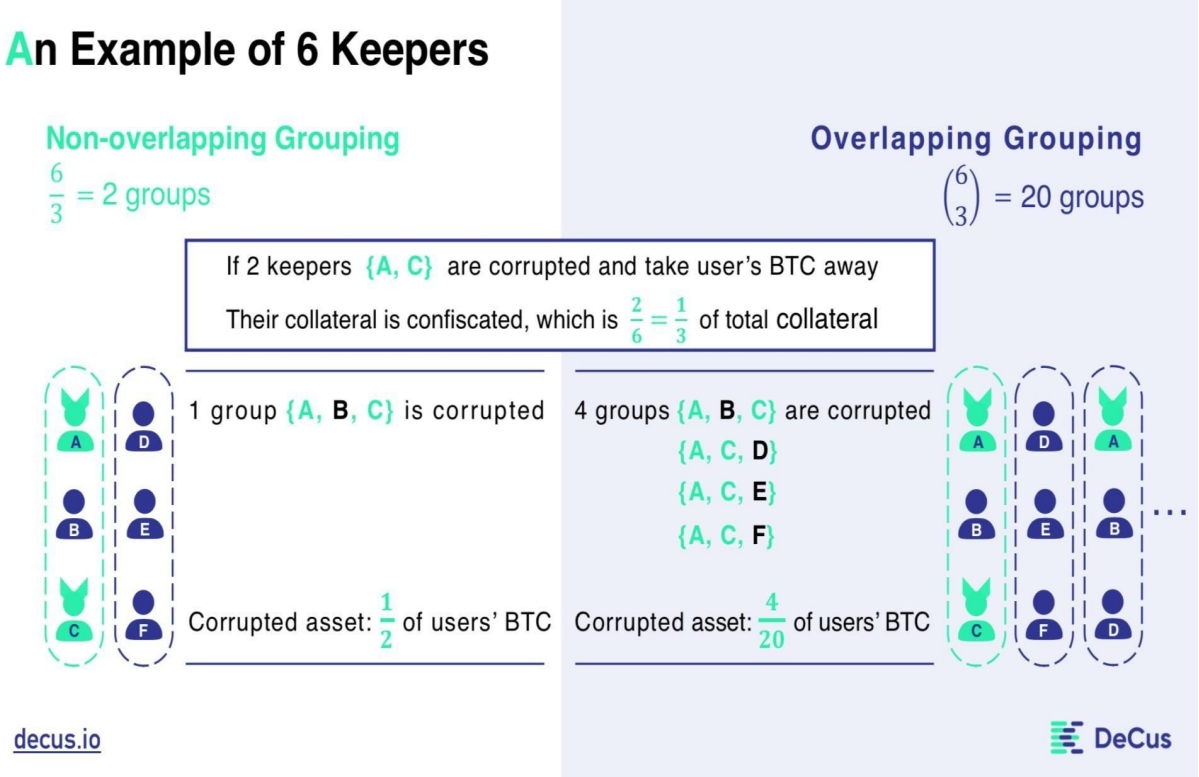
Users may then convert their eBTC back into BTC at any time. The redemption process is essentially the same as the minting process. Once the original BTC has been received back, the corresponding eBTC is be burned.

What is the underlying method?

A decentralized and self-regulated Custodian Network based on Dr. Yang Guang's cryptography IP is the cornerstone of the whole system.

Suppose that the BTC assets are kept by 10,000 Keepers in a multi-sig address for which every transaction needs at least 5,001 signatures. As long as the majority of Keepers remain honest, an adversary could not steal any BTC under custody. In this case, a minimum collateral would be sufficient to enforce compliance among the Keepers.

However, securing and verifying confirmations from 5,001 of 10,000 multi-sig address would be quite technically challenging for the Bitcoin network.



The key then to balancing the security provided by large groups and the accessibility offered by smaller groups, DeCus uses an innovative custody scheme based on overlapping group assignments. The following example can demonstrate how it works.

Suppose there are six Keepers partitioned in two 2-of-3 multi-sig groups each of three Keepers. Then by corrupting two Keepers the adversary is able to get full control of one group, which is 1/2 of the total assets under custody.

Alternatively, let's enumerate all 2-of-3 multi-sig groups drawn from the six Keepers. There are 20 groups in total, whereas by corrupting two Keepers the adversary only controls four groups (each corrupted group consists of two corrupted Keeper and another honest one). Thus, the same 1/3 fraction of adversary only controls 4/20=1/5 of all groups. In other words, the new scheme is able to securely keep 5 BTC with total collateral of 3 BTC against 1/3 adversary, since the profit that could be gained by launching an attack is less than the adversary's collateral.

Of course, the above example is designed for illustration purposes but not for showing impressive collateral efficiency. We can estimate the ratio of collateral to total assets under custody asymptotically as follows:

1. Suppose the total assets under custody is A and there are n custodians.
2. Suppose the total collateral is C and the fraction corrupted custodians is γ. Thus the collateral of adversary is $\gamma \cdot C$ when every custodian provides the same amount of collateral.
3. Suppose the custodians are assigned to all possible 4-of-7 groups. There are $\binom{n}{7}$ such groups in total.
4. The probability of a single 4-of-7 group being corrupted is roughly
$p_{corrupt} \approx \binom{4}{7}\gamma^4(1-\gamma)^3 + \binom{5}{7}\gamma^5(1-\gamma)^2 + \binom{6}{7}\gamma^6(1-\gamma) + \binom{7}{7}\gamma^7$
$= 35\gamma^4(1-\gamma)^3 + 21\gamma^5(1-\gamma)^2 + 7\gamma^6(1-\gamma) + \gamma^7$
5. For $\gamma < 1/2$ (and hence $\gamma < 1-\gamma$) the above probability is bounded as follows
$p_{corrupt} < 35\gamma^4(1-\gamma)^3 + (21+7+1)\gamma^5(1-\gamma)^2 = 35\gamma^4(1-\gamma)^2$
6. The custody scheme is secure if the amount of assets controlled by adversary does not exceed adversary's collateral, i.e. $p_{corrupt} \cdot A \leq \gamma \cdot C$.
7. Therefore, it suffices to have $64\gamma^4(1-\gamma)^3 \cdot A \leq \gamma \cdot C$. That is, the collateral ratio is $C/A \geq 35\gamma^3(1-\gamma)^2$.
8. For $\gamma = 0.2$, the right hand side of above inequality is 0.1792, which means the collateral can be less than 20% of the total assets under custody. Significantly improved from 150~300% over-collateraliation!

For small γ, the collateral ratio decreases in $\sim \gamma^3$. For groups requiring more participants to sign, say 5-of-7 or 5-of-9, the collateral ratio decreases even faster in $\sim \gamma^4$. In particular, the collateral ratio of 5-of-7 groups against $\gamma = 0.2$ adversary the collateral ratio is bounded by 3%.

Based on the above analysis, DeCus is able to implement its decentralized custody scheme with fewer groups represented and while achieving an impressively low collateral ratio. For example, with a polynomial design over prime fields, DeCus is able to achieve an efficiency factor of η=A/C of as much as 20 with n=121 Keepers, which means the collateral is <5% of total assets under custody!

Who are the Keepers? Can anyone become a Keeper?

Keepers are responsible for the custody of underlying crypto assets. All keepers are organized under the overlapping group assignments in a 100% decentralized way , and are required to deposit collateral in order to ensure compliance.

DeCus will soon launch a permission-less Dutch Auction to select the first batch of Keepers. Anyone who is interested in being a Keeper can participate in the auction without any KYC or AML.

Once the system has undergone several rounds of testing and enters the mature phase, Keepers will be allowed to join or leave at their leisure. For every new user deposit, a new Keeper group is pulled together and constructed (selected at random), and a new Bitcoin multi-sig address is generated for the depositor, which is marked on the Ethereum chain.

Why do we launch a Dutch Auction? How does the Dutch Auction work?

The stable operation of system relays on Custodian Network. If the number of Keepers istoo small, the whole system will become insecure. So we need an efficient and fair way to initiate a bootstrap process of the Custodian Network. Under current circumstances, Ductch Auction seems to be the best way because of two features: 1) Permission-less, which means anyone who wants to be a Keeper can participate in the auction; 2) Transparent, which means all participants can compete fairly under the set rules; 3) Participation discovery, which means the real willingness to become a Keeper can be figured out through the whole process.

During the auction, candidates need to set the amount of deposit they would like to commit, according to which the system will rank in real time. By the end of the auction, the top n will be selected, with the n-th committed deposit amount being used as the final deposit amount for each selected keeper. During the auction stage, the deposit can be retrieved at any time. Once auction ended, the mint stage will launch at which the Keepers' collateral will be migrated to the Vault of Custodian Network and each Keeper operates his/her node of the Custodian Network.

How can a Keeper benefit from the system?

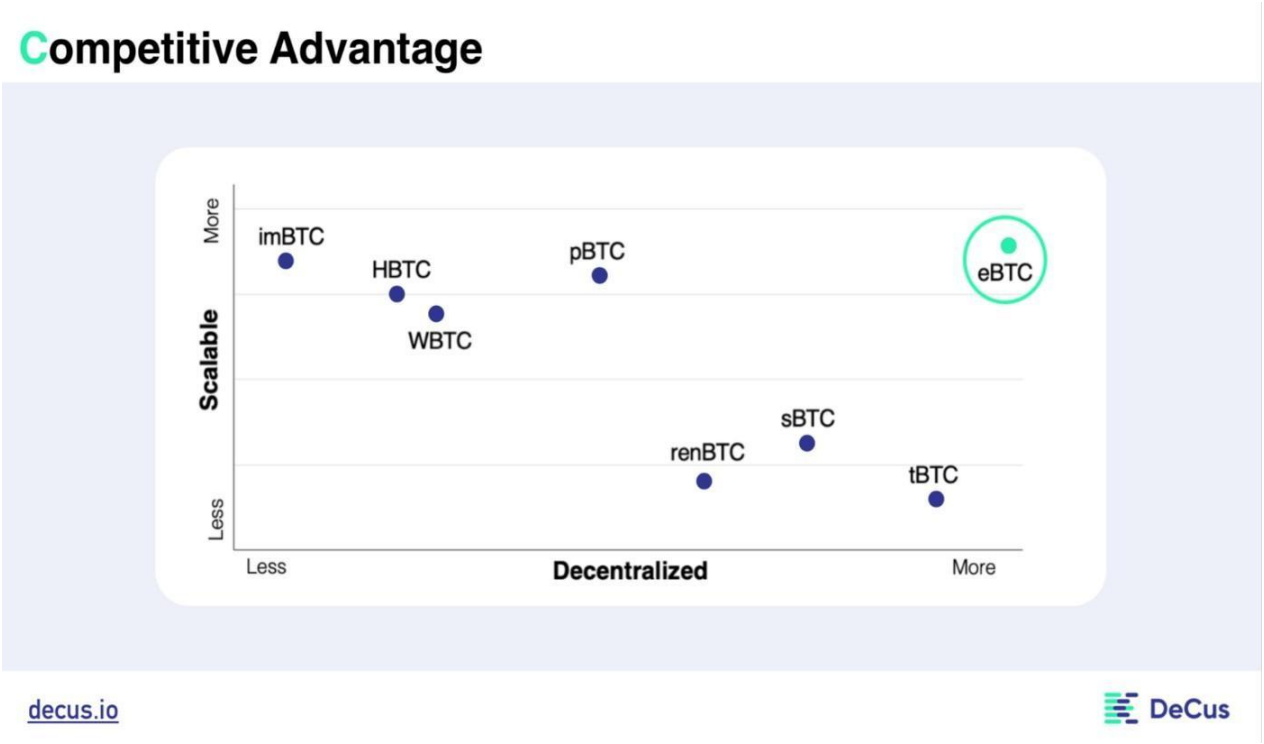
As the core role and long-term partners of the whole system, Keepers will receive 3 types of benefits: 1) a share of system revenue, which is generated from the fees of eBTC (or other pegged value crypto assets) minting and redemption; 2) collateral interest, namely the deposit interests for Keeper collateral, as eBTC is the first tokenized bitcoin that shares such interest to the custodial party of the underlying assets; 3) farming yields, which will be generated by integrating crypto collaterals into yield farming protocols such as Curve, Compound and AAVE etc.

Why is eBTC better than other tokenized bitcoins?

Decentralization and scalability are well balanced by eBTC as compared to other tokenized bitcoins.

Some tokenized bitcoins, like WBTC and HBTC, are issued by a centralized party, so they may become irredeemable in case of a single point failure or censorship.

Other BTC-backed tokens, such as tBTC and renBTC, are issued in a decentralized way. However, they rely on a high collateralization rate to mitigate the risk of price fluctuation and misbehavior. For example, each minted tBTC-token requires collateral of value ≥1.5BTC, and each renBTC requires collateral value ≥3BTC. Such over-collateralization would significantly increase the cost of using tokenized bitcoins.



eBTC gives a different answer. The decentralized and self-regulated Custodian Network of the system enables eBTC implementation at a much lower collateralization rate, with 30%-50% compared to the average more than 150% of other solutions, while still beingdecentralized.

DeCus token overview

Supply: 1,000,000,000 (1 billion)

Functionality: Governance

Name: DeCus - DCS

Allocation

1. Participant Incentive - 45%

Mint Mining - 25%

- For each eBTC minted, both keeper and minter are rewarded
- One year or 6-month linear vesting

Liquidity Mining - 10%

- Collaborate with other protocols, broaden the usage on other applications

Keeper Collateral Mining - 10%

- Minimum incentives for keepers when mint mining is slow
- We encourage keepers to use EBTC as collateral, to improve weight in mining
- One year or 6-month linear vesting

2. DAO Community/Infrastructure - 15%

To be decided by the DAO - 15%

3. Early Investors - 18%

For investors in Rounds 1, 2, 3; vesting via accelerating schedule over 2 years

Maximum 25% every 6 months

Incentive1: The higher the proportion of mint to the total mint, the higher the unlock rate (e.g., the rate of unlock will be 5% more for a 1% higher proportion of mint)

Incentive 2: If X tokens are purchased from the marketplace and locked, an extra 1% will be locked from that point (e.g., if investor A locks 10000 tokens, an extra 100 DCS can be unlocked 100 days after that point)

4. Core team - 15 %

5. Auction & Booststrap - 7%

Mainnet test round: 0.5%

Each auction round: 0.5%, 1%, 2%

Initial trading rewards (Uni, Sushi, DODO) - trading/mm: 1% each

Profit sources

1. Mint/Burn Fees

Total minted eBTC <= 10000

- Mint: 0%
- Burn: 0.2%. Burning fee should prevent Mint <=> Burn arbitrage.

Total minted eBTC > 10000

- Mint: 0%

- Burn: 0.2%

2.Keeper Participation Fees

- In: 0%
- Out: 0.5%
- In the auction phase or early stage, keepers are not allowed to leave

3. Keeper Collateral Financing

- Partnerships with other DeFi protocols, for a fixed-rate income of keeper's collateral asset (e.g., risk-free lending protocols, fixed-income protocols)
- Incentives: collaterals are just viewed as a safe-guard to prevent keepers from doing any harm to the protocol. As long as the protocol has ownership of the collateral and uses it without any losses, more profit is generated for the protocol
- This feature will not be launched initially but will be enabled once the core protocol is stable

Profit distribution

1. Mint/Burn Fees and Keeper Participation Fees

- Keepers - 70%

- Keepers share cash profits from all commission fees

- DeCus Stakeholders - 30%

- Phase 1: rebate cash profits for staked DeCus tokens (tokens locked in the protocol).
    - Initially, there will be very few usecases for DeCus token. But, the protocol will share cash profits with DeCus stakeholders.
- Phase 2: DAO community will take control of the profits once the DAO is formed

2. Keeper Collateral Financing/Investment Strategy

- Keepers - 90%
- DAO - 10%
- DAO have the rights to adjust the proportion

Who built DeCus?

DeCus was built by a group of decentralization believers and DeFi natives with prior years of developer experience at leading companies both in the Internet and the blockchain, with theoretical research being led by a team of Phds from several of the world’s top computer science and cryptography universities.