BESS

Bess Protocol White Paper

Layer 2

The new generation of DEX

V1.0

Abstract

At present, the cryptocurrency market takes on a great deal of speculative attributes where participants are not content with such spot transactions as currency exchanges. Derivatives trading can amplify capital utilization and hedge potential risks for investors. This alone appeals greatly to investors in cryptocurrency. In addition, the prosperity of the derivatives market is an important measure of a mature financial market.

In the traditional financial market, the market size of derivatives transactions is 40 to 60 times that of spot transactions. However, there has not been a significant gap in the turnover between derivatives and spot transactions in the cryptocurrency market. Therefore, many practitioners believe that crypto derivatives still have a lot of room for development.

From the perspective of the DeFi ecosystem, the DeFi ecosystem has gradually developed fully. MakerDAO has played properly the role of a decentralized central bank. Aggregate mining protocols such as Yearn can effectively improve the utilization of funds. Insurance projects such as Nexus Mutual can improve the security of funds. Such DEX as Uniswap have effectively assumed the role of facilitating token exchanges, whereas the decentralized derivatives trading pattern as an important part of the DeFi ecosystem remains underdeveloped. With further improvement of the Layer2 technology, derivatives trading will usher in explosive development, and Bess Protocol (hereinafter referred to as Bess) will also become one of the most representative projects.

1. What is Bess?

Bess Protocol is a Layer2 decentralized derivatives trading protocol based on the Rollup technology for capacity expansion. It is a versatile decentralized exchange (DEX) to be built on the Ethereum. Using a decentralized custody scheme for asset transactions, it accommodates futures, options and related derivatives, etc.

The Bess token is a license for transactions on the platform, which is proportional to the ownership percentage of the token supply and charges no agreed protection fee. At the same time, anyone can add liquidity and obtain considerable market-making income by depositing collateral in the AMM pool of the Bess protocol. It also subsidizes slippage loss in real time through Bess protocol tokens to ensure user benefits. Integrating the liquidity of mainstream DEX and CEX, the transaction process has better transaction depth and faster transaction response and is entirely completed autonomously through the smart contracts on the blockchain.

In the future Bess will not be limited to cryptocurrency. Any asset such as cryptocurrency, gold, fiat currency, etc. (whether it is cryptocurrency or non-cryptocurrency) can be traded with up to 100 times leverage and cross margin. It also provides traders with the trading experience similar to CeFi. Based on Rollup's Layer2 technology Bess offers low latency and high speed in transactions, reducing the risk of delay. A plasma variable designed for transactions will also be introduced in subsequent compilations to achieve trusted non-custodial transactions.

2. Imagining with Bess Protocol

Currently, the scale of digital asset transactions is experiencing explosive growth, and the scale of derivatives transactions on centralized trading

platforms has surpassed that of spot transactions by a large margin. However, when will derivatives trading reappear or even go beyond the imagination of traditional financial markets on decentralized trading platforms and give birth to new unicorns? This is something worth expecting.

Generally speaking, derivatives can better meet market participants' demand for advanced asset allocations with higher volatility or risk hedging. Although spot commodities allow risk management through combinations, from the perspective of the entire capital market, the basis for continuous capital valuation and capital conversion is lost, and the efficiency of capital circulation will significantly decline. From the perspective of financial laws, in terms of liquidity and transaction scale, derivatives transactions are greater in volume than spot transactions.

Bess in the future will not only satisfy the derivatives trading for assets, but also accommodate the trading of all things. Through more flexible and pragmatic methods, it will bring the masses of mainstream traders into the decentralized finance (DeFi) world.

3. What Problems Does Bess Protocol Solve?

In fact, there are such DeFi ecosystems as dYdX, Opium and other derivative exchanges, but these exchanges have more or less flaws. For example, dYdX also relies on the lender's tokens for lending and then users who want to go long or short pick desired orders from the order book, but the efficiency of this operating system raises questions. Moreover, the stampede effect caused by the quotation system and slippage is also worrying.

In DeFi, the role of market maker that provides liquidity will be played by users, which means that the idle funds have a way out and the overall efficiency of the use of funds in DeFi will be improved, but this is unlike composable DeFi

that despite high rewards must bear the potential high risk of stacking all components. On the DEX platform, liquidity is dispersed into different agreements. Insufficient market-making liquidity of the AMM will cause greater slippage. At present, most DEX platforms lack sufficient trading tools, causing poor user experience and putting off institutional investors.

Current DeFi seems to lack an effective derivatives exchange, and the emergence of the decentralized derivatives trading protocol Bess, in a sense, better complements the DeFi ecosystem.

Unlike the above-mentioned derivatives exchanges, Bess does not adopt an order system, but takes external quotations to completely solve the problem of slippage. Then, through the reward mechanism of liquidity mining, the overall liquidity is improved, thereby improving the overall transaction efficiency, which opens up the horizon for derivatives.

In its plan, Bess hopes to be more secure and equitable than traditional centralized exchanges and to offer a better experience than existing decentralized derivatives exchanges. In the future, there will be more options for trading targets, which coupled with the multi-facet advantages in leverage ratio (capital use efficiency), handling fees, gas (transaction fee), and cross-platform transactions, paves a practical highway for investors in the DeFi world.

4. The Trusted Model of Bess Protocol

4.1 Uncertainty of centralized exchanges

When a user deposits tokens into his deposit address, in a sense, he gives up the supervision of the exchange and can retain ownership only when the exchange completes the grant action. This way may easily cause the loss of

tokens due to malicious intention or incompetence of external exchange personnel.

Centralized transactions provide a very low level of security. Transaction links could become attack nodes through various simulations and access swaps for identity verification and account association. However, the complexity of the transaction links indicates high uncertainty in networked node transactions.
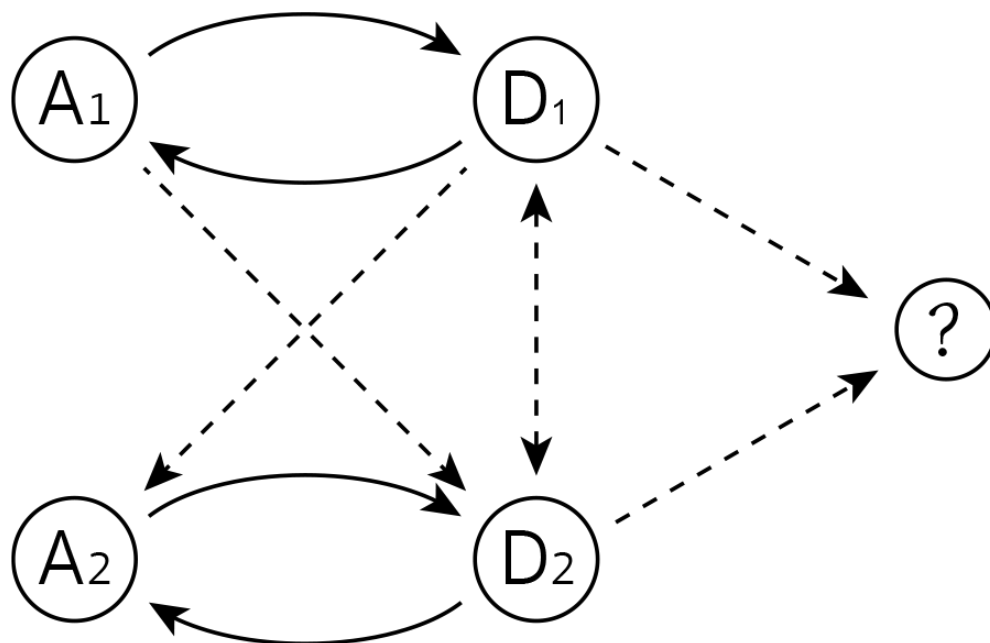

Figure 1: The flow of user funds in various addresses is indicated at the time of centralized exchange. For example, there is no restriction on the flow between A1 and the deposit address D2, which makes security validation infeasible.

Centralized cryptocurrency exchanges have no way to prove that they are not operating or misappropriating customers' assets. Many centralized exchanges in the cryptocurrency industry do not have reserves as traditional asset trading platforms do. Therefore, once the exchange is insolvent, users will suffer

severe losses of assets. In addition, the theft, loss, and misappropriation of assets in many centralized exchanges are usually not immediately discovered, so operators may continue to operate the exchange's funds without the user's knowledge.

Due to the lack of open, transparent and verifiable integrity checks, no practical measures could be taken to identify a malicious operation. In short, any major transactions and asset security on a centralized cryptocurrency exchange are beyond the control of users deprived of ownership of their own assets.

4.2 On-chain Exchanges (DEX)

The interactions on the blockchain allow the blockchain to easily constrain the exchanges.

Most of the heavy work is done through the network and publishing block transactions. Early decentralized transaction models can be run solely on the blockchain because they have order books and smart contract's token reserve to interact with users. Users can trade freely in the blockchain network and have initiative over their own property.

Although currently the transaction cost and speed have increased due to the emergence of gas, the technological development of Layer2 will make the transaction process more convenient and faster. Users can also manage and take care of their own assets under the premise of the wallet security and have a more intuitive experience during transaction through the interactions between blockchains.
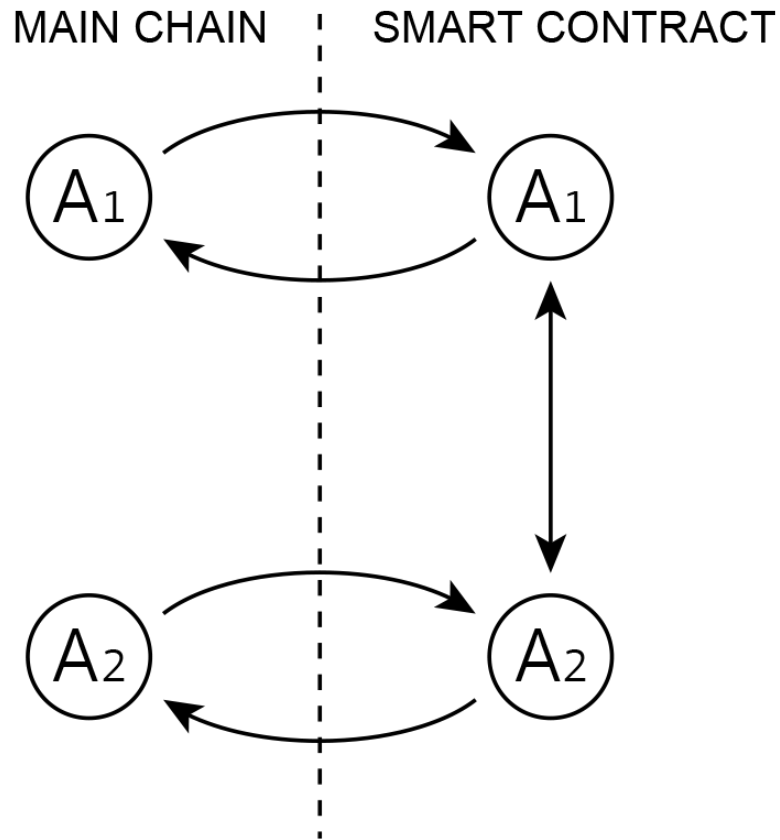
Figure 2: DEX ensures security by synchronizing across the chains to both ends of the blockchain, but it is currently limited in scale and transaction delay. With the time restricted by potential blockchain transactions per second and confirmation on the chain, usually an unhackable level is reached.

4.3 Estimating option prices under the influence of volatility

At present, many option markets for digital currencies are not perfect. Therefore, we cannot calculate the implied volatility of the market from the option price. We should use the volatility history and the sample standard deviation as a proxy for the true volatility. Since there is no oracle network to provide historical volatility data, the Bess protocol needs to use the option data history obtained from authoritative oracle solutions such as Chainlink and calculate it by itself.

Compared with the option data collected by centralized exchanges, due to current technical limitations, the data provided by Chainlink is less organized. Therefore, we need to ensure that the option volatility does not postpone the expected price for a series of non-technical reasons and that those errors do not affect the volatility estimation process. To this end, we will extract a part of the chained data to achieve a volatility estimator in the following way.
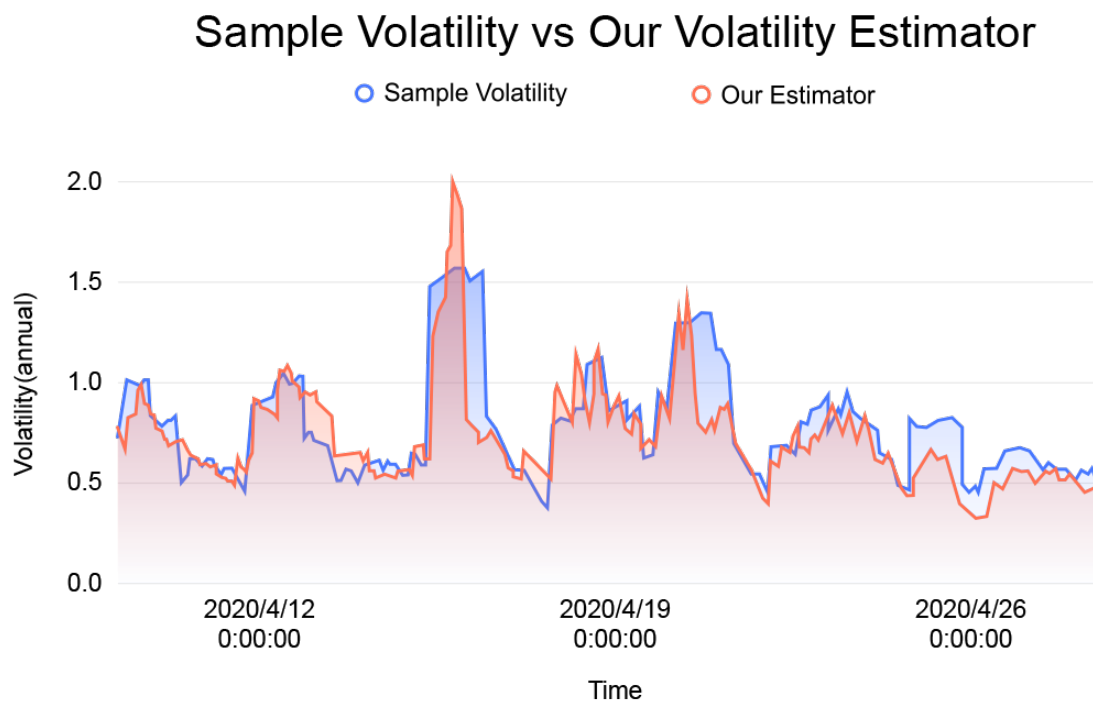

Figure 3: Blue line: A volatility sample calculated from the hourly USD/ETH exchange rates collected from Binance for a certain period of time. Red line: An estimation model based on the unevenly spaced data collected from Chainlink.

Volatility Estimator

=std (latest 24 percentage differences) x $\sqrt{(\text{One year}) / (\text{Elapsed Time})}.$

The formula also shows that if any FX option data can be obtained at the same time interval, this approach of volatility estimation may offer certain reference value. However, in the actual trading process, there will not be a theoretical constant value for the prices of each interval, but there will be uneven fluctuations.

Therefore, in order to achieve an effective estimation model more accurately, Bess will generate a weighted average that calculates the squared difference, where the weighted average is marked as a function of the elapsed time of each data point. Therefore, such an effective volatility estimation model has reference value and certain anti-risk attributes.

4.4 Order book for sub-accounting

All transaction and order state changes are recorded in a ledger so as to verify the balance, source and validity of each transaction. Independent of another sidechain, Bess keeps the core of the transaction states in its own ledger, which can also be regarded as a zero-knowledge proof of Bess independence.

Field	Meaning
Entry ID	ID for the new state
Prior Entry	Prior state
Type	Origin, Deposit, Trade, Fee, Withdraw, Excited
Account	Ethereum public address of owner
Asset	Token Address. All zeros from Ethereum
Quantity	Net Change from prior balance
Balance	New balance
Witness	Acceptable Proof of validity

The Bess ledger has six types of entries: origin, deposit, withdrawal, exit, and two transaction entries. The initial state, also known as Origin, is a special entry system that records universal zero balance. The deposit and withdrawal entries run on different smart contracts.

State	Prior	Type	Account	Asset	Qty.	Bal.	Witness
0	0	Origin	*	*	0.00	0.00	
1	0	Deposit	A_1	Z_1	+0.10	0.10	Deposit Harsh
2	1	Trade	A_1	Z_1	-0.05	0.05	Orders, Fill
4	0	Trade	A_1	Z_2	+0.02	0.02	Orders, Fill
5	3	Withdraw	A_1	Z_2	-0.01	0.01	Prior balance
5	4	Exited	A_1	Z_2	-0.01	0.00	Exit Block

For the state transition of each account there is enough data to prove the correctness of the transaction process and the details of various transaction states. The table shows the transaction states from depositing asset Z1, converting 0.05 of it into 0.02 of asset Z2 to finally withdrawing and exiting to account A1.

The change and update of this set of transaction data will uniquely have the dual signatures of all parties and of the operators which will be copied continuously in the network according to demand. The new state replaces the old one to complete the replication. In other words, the balance of State 2 (A1; Z2) completes the consumption interaction and balance transfer of the asset through the update of State 6. Further transactions of the same asset update the existing balance to the new state.

5. Team Composition

Bess is headquartered in Singapore. The team comprises senior product managers from world-renowned banks, futures companies and leading exchanges, core developers of well-known public blockchains, and a group of geeks majoring in computer science that graduated from such top universities as Carnegie Mellon University, Stanford University, University of California Berkeley, etc. The team boasts extensive experience in cryptocurrency industry and in development and design of traditional financial products.

6. Bess Protocol Conception

In the first version launched by Bess, users can stake ETH, WBTC, mainstream stablecoins, Bess (Bess's platform token) and other major ERC20 tokens in smart contracts, mint BSDT (Bess platform's stablecoin), and then implement piggyback transactions on the Bess platform through Rollup's Layer2 solution. On the premise of the security, the funds are locked in smart contracts and are all open and transparent.

Bess will balance user experience and transaction performance on the basis of decentralization. It is positioned as the "Uniswap" in the field of derivatives trading, aiming to help users get back control of assets and pursue various traits such as decentralization, automatic market making, and composability. Compared with centralized exchanges and other DeFi derivatives, Bess features automatic market making, external price feeds, real-time subsidy for slippage, and support for cross-chain exchanges. In the future, it will further implement the brokerage arbitrage model and launch investment decision-making tools. It is worth noting that Bess does not provide extremely risky binary options whose strike price is set at the current market price.

In the next step, Bess will enrich its product library from two aspects: 1) to increase blockchain parameters of existing derivatives; 2) to build more abundant derivatives. Furthermore, Bess will continue to explore the pricing

model that eliminates the oracle and to develop derivatives based on the characteristics of Ethereum 1.0 and Ethereum 2.0 (and its transition period).

7. Token Model

Configured as a smart contract platform on the blockchain, Bess Protocol is mainly divided into the following two smart contract modules:

Bess smart contract: Mainly responsible for the locking, issuance and conversion of Bess tokens; BSDT stablecoin smart contract: Responsible for issuing and managing BSDT tokens, maintaining price stability, supply and tracking, and helping control the supply in the entire system through additional destruction and issuance.

The BSDT stablecoin is not only the very core part of the entire Bess Protocol, but also a voucher for value conversion between different chains. Users conduct value transactions, staking, and even liquidity mining through BSDT. According to the Bess Protocol consensus algorithm for exchange rate, the equivalent number of tokens is output. The tokens between different chains can be exchanged in value. Equivalent exchanges can be made to obtain timely liquidity through Bess Protocol.

Therefore, as more and more asset classes are tokenized, the investment portfolio will gradually change from simple to complex over time. Bess will also increasingly manifest its unique value.
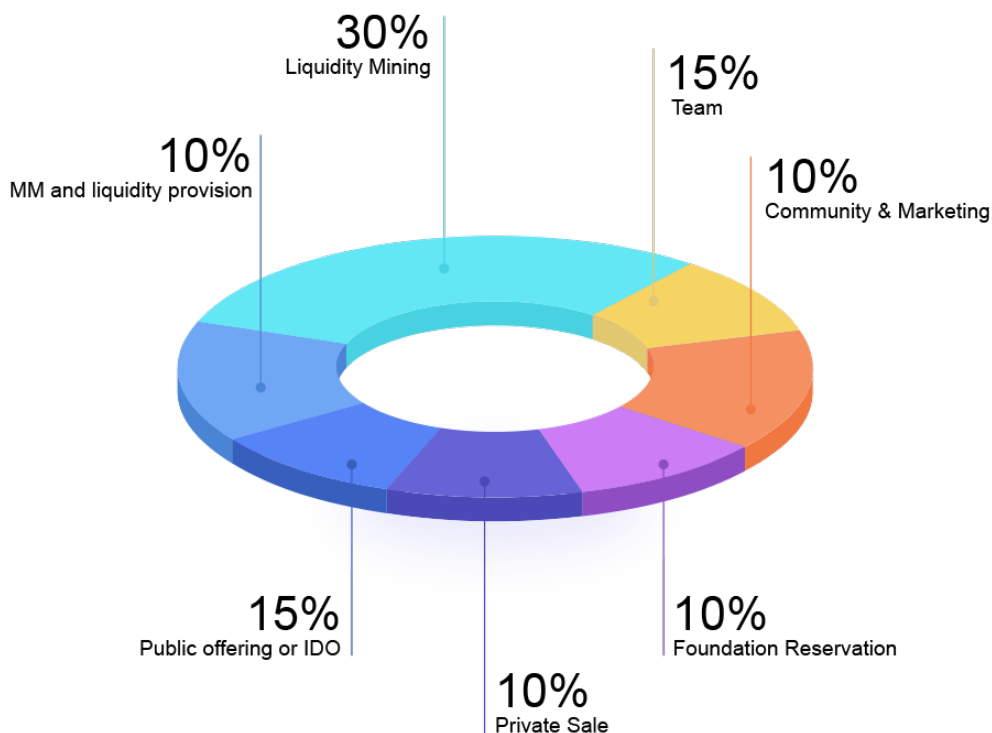
Initial Supply: 10,000,000 BESS

Team: 15%

Tokens reserved for team are fully locked for 6 months and will be released by 5% monthly thereafter.

Community & Marketing: 10%

These tokens are assigned to individuals and groups that develop core tools and infrastructure on Bess Protocol and support Bess Protocol through grassroots community building and marketing. The tokens will be released according to the actual conditions of promotion.

Foundation Reservation: 10%

Tokens reserved for foundation are fully locked for 12 months and will be linearly unlocked quarterly over 3 years. Bess Protocol is used for project planning and construction and cooperation with external projects.

Private Sale: 10%

10% of the tokens sold in the Private Round are released before the locking. The remaining 90% will be distributed monthly over one year.

Public offering or IDO: 15%

Fully unlocked with no restrictions.

Liquidity Mining: 30%

The rest will be gradually released as a reward for liquidity mining.

MM and Liquidity provision: 10%

As the provision of liquidity in DEX and CEX.

8. Legal Terms

This document is a technical white paper for information purposes only. It is not a statement of future intentions. The content of this document and the Bess Protocol project may be changed, so please subscribe to email updates on our website to be notified when the website changes. Unless specifically stated otherwise, the products and innovations mentioned in this document are currently under development and have not yet been deployed. Bess Protocol does not make any guarantee or statement regarding the successful development or implementation of such technologies and innovations or the success of any other activities mentioned in the document. Nor does it assume any guarantee implied by law or other means to the extent permitted by law. No one has the right to rely on the content of this document to make any inferences derived therefrom, nor has any right to interact with Bess Protocol or the technologies mentioned in this document.