TideBit

Technical Whitepaper
of Hong Kong Cryptocurrency Exchange

TideBit v2.0.4 20230323

CONTENTS

TideBit

01

Background

Fintech Nowadays

In recent years, the rapid development of financial technology has attracted many companies to invest. According to reports, the total investment in the global Fintech industry reached 210 billion US dollars in 2021, with record trading volumes in major markets such as the Americas, Europe, the Middle East, Africa, and the Asia-Pacific region. Among them, blockchain and blockchain assets are the most most stand-out, bringing huge changes to modern finance.

Since the emergence of Bitcoin in 2009, blockchain assets have gradually entered the investor's field of vision, among which Bitcoin, which has skyrocketed more than 20 million times to date, is the most popular and has attracted a large number of investors' attention. The characteristics of the volatile rise and fall of cryptocurrencies have prompted central banks or related agencies in various countries to introduce various regulatory policies. As cryptocurrencies are still comparatively small in market capitalization compared to the global traditional financial market, many people have realized its growth potential, hence hold an optimistic attitude towards the future of cryptocurrencies.

In addition to Bitcoin, which is already well-known, the development of Ethereum, which has risen more than 15,000 times through crowdfunding, cannot be underestimated. Ethereum has Turing-complete features and smart contract functions that can automatically execute transactions, creating a large ecosystem. At the end of 2015, Ethereum established the Ethereum token standard. Through the ERC20 standard-designed tokens, smart contracts can be used to exchange and circulate tokens. This has also stimulated innovative fundraising methods such as token issuance, opening the prelude to a new era of token economy.

According to the guidelines issued by the Swiss Financial Market Supervisory Authority (FINMA) in February 2018, tokens are defined as three types: payment tokens, utility tokens, and asset tokens. The tokens launched by cryptocurrency exchanges belong to the category of utility tokens, only providing the right to use exchange services or applications. Since platform coins belong to exchange-specific use, with the increase in transaction volume, their usability is high, and their value is stable. Therefore, there is much anticipation for their appreciation potential.

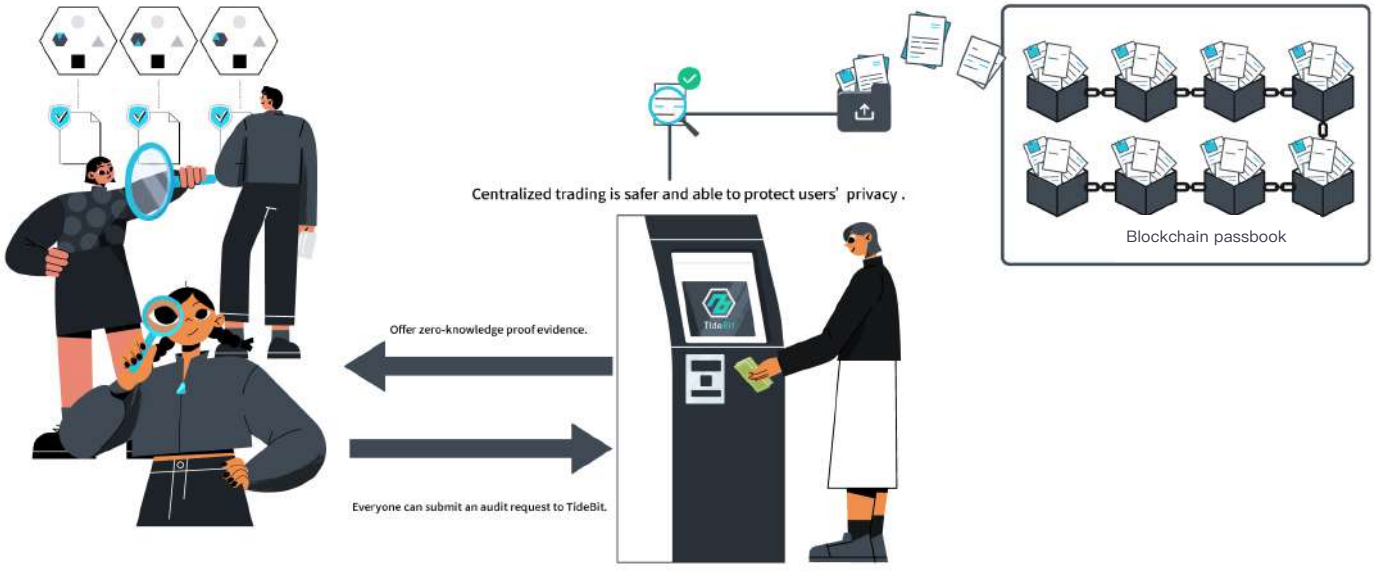
Today, with the development of financial technology, digital payment is also booming, gradually replacing cash transactions. In order to cope with more and more innovative applications of financial technology, central banks around the world have also begun to actively study the feasibility of digital currencies. However, each country's attitude and development strategy towards CBDCs are very different. Among them, China is positive, while the EU does not guarantee that it will issue a digital euro in the future.

Financial technology is steadily and effectively changing the operating mode of global society. However, the social system often cannot keep up with the rapid changes brought about by technology, which has led to problems.

Challenges of Regulation

Technologically speaking, there have been frequent cases of international large exchanges being hacked, and many users' encrypted currencies stored in exchanges have been stolen by hackers and cannot be recovered, causing significant losses to users and exchanges. However, such incidents often cannot trace the culprit, nor can they provide reasonable compensation to the victims.
In terms of the system, we have experienced the bankruptcies of Wirecard, a German payment company, in 2020, Greensill Capital, a financial technology company, in 2021, and FTX, the world's second-largest cryptocurrency exchange, in 2022. We found that in addition to the lack of effective regulatory mechanisms for emerging financial technology services such as blockchain asset exchanges, traditional financial services also reflect that existing regulatory systems are inadequate to cope with new era financial services.
Although companies in the Fintech sector are more innovative than traditional financial institutions and more willing to adopt new technologies to solve past problems, they face greater risks and uncertainties as a result. Therefore, with the advancement of governance concepts and technological development, Fintech companies and regulatory authorities should fully utilize new technologies to optimize their business models and risk management measures. The TideBit team has proposed a solution (as shown in Figure 1) that combines centralized trading with decentralized supervision to address potential risks and challenges posed by the continued progress of Fintech in the future.

Figure 1



Combination of centralized trading with decentralized supervision

History of TideBit

TideBit was launched in 2017 as a centralized exchange registered and compliant in Hong Kong that supports both fiat currency and major blockchain assets. TideBit's clients primarily come from local Hong Kong retail and institutional investors, with a high level of cultural knowledge and a keen interest in investment. Currently, TideBit has approximately 60,000 regular users, and has actively complied with government regulations since its launch in 2017. TideBit will further expand to Sun TV viewers and global Chinese communities. TideBit is also actively involved in the research and development of blockchain auditing and security technologies, and holds multiple underlying operation and risk control technologies, maintaining zero incidents of intrusion and zero abnormal disasters to date.

02

TideBit 2.0 Overview

DeNA –
Decentralized Identification and Asset Protection

Decentralized identity verification is an identity verification mechanism that aims to verify the identity of participants without the need for a third-party authoritative institution. This mechanism is based on blockchain technology, using encryption algorithms and decentralized storage to ensure that participants' identities and data are not tampered with or counterfeited. TideBit's decentralized identity verification is based on blockchain identity, using distributed ledger technology and encryption algorithms to assign unique digital identities to participants. Each digital identity can be bound to one natural person or legal entity identity, and each binding has been audited and certified by TideBit. This identity can be used to verify the identity of participants in decentralized applications, and even participate in public affairs decision-making.

Decentralized Regulation

Many people have a common misunderstanding about blockchain, which is that because blockchain is decentralized, it is impossible to coexist with regulatory entities that are themselves a huge centralized authority. At first glance, this argument seems to make some sense, but it is actually not right because decentralization does not mean the absence of a center, but rather emphasizes fairness and freedom among many centers of different sizes.

In fact, the concept of decentralization has never aimed to eliminate or deprive the center of its rights since its inception. Whether it is Bitcoin or later blockchain technologies, their goal is to avoid a powerful centralized control by only few people, instead of excluding or eradicating the center.

A decentralized system is a distributed network composed of many centers of different sizes. In the proof–of–work mechanism of Bitcoin, even the large computing power mining pool is actually a large center, and both large and small miners must follow the same rules of more work and more rewards to avoid the unfair distribution of rewards caused by the control of the entire system by a large center.

Therefore, in the future, under similar fair mechanism conditions, as more and more people recognize and accept them, large organizations, even some countries, can freely become members of countless nodes and be treated fairly by the system so the decentralization and central organizations can coexist.

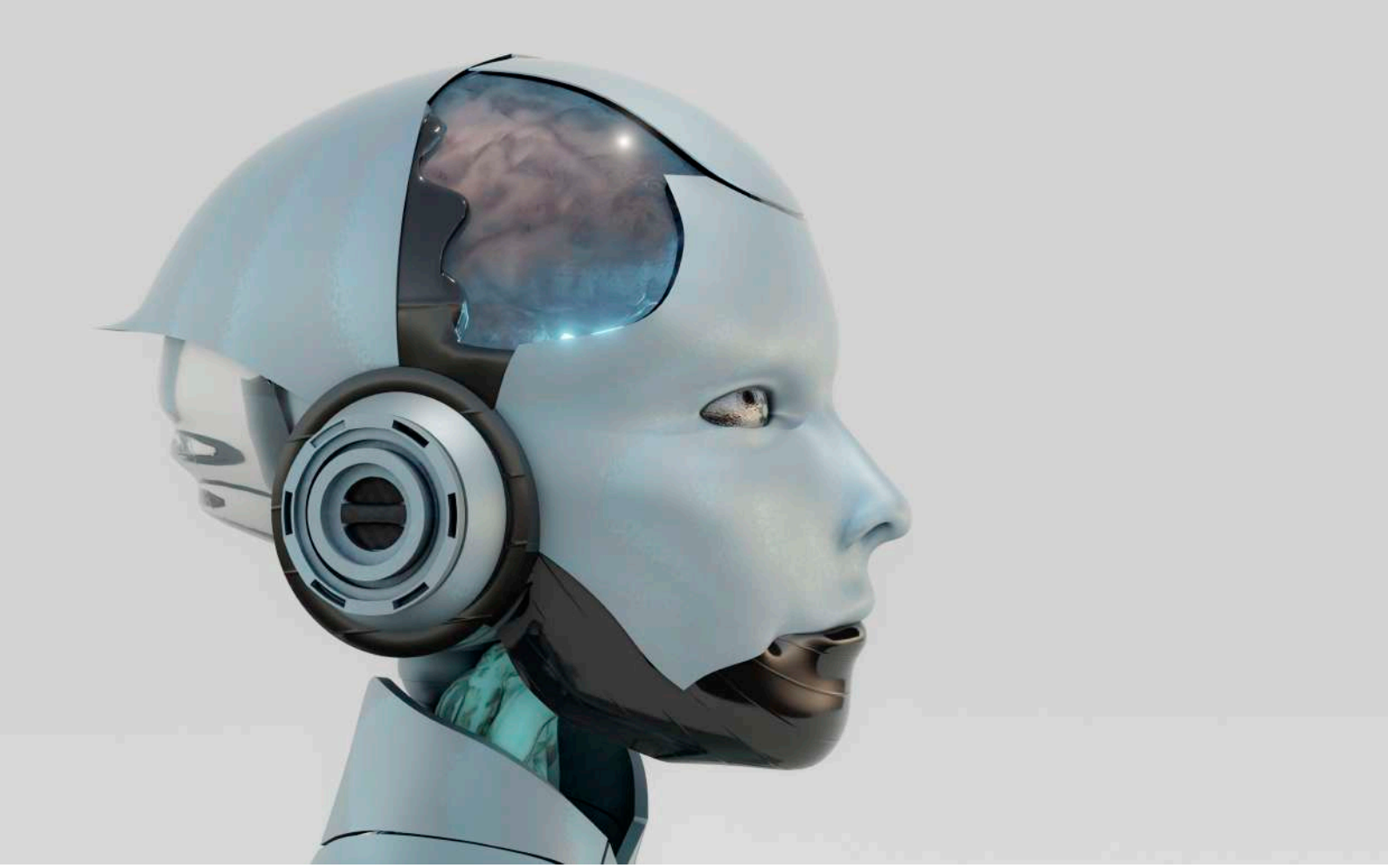
Decentralized networks seem can offer equality to all individuals, allowing them to act freely without anyone to oversee them, much like the anonymity of the early days of the internet was often used for unlawful behavior. As technology rapidly changes people's lifestyles, regulation often lags behind. The speed of technological development is very fast, and no one can know where it can take us to. Even large organizations may not be able to grasp the most advanced technological developments and can only follow the pace of development to do things that maintain social stability while not hindering scientific and technological development. Under this premise, it is unrealistic for a small number of organizations (such as the government) to carry out regulation, so we need different regulatory models.

With the development of blockchain technology, especially zero-knowledge proof technology, the form of open data has become more diverse. Validating a piece of data no longer requires exposing all the data to regulatory agencies, but instead submitting encrypted and compressed evidence data regularly. When specific range data is questioned, decrypted plaintext data can be submitted for verification and compared to the evidence on the blockchain.

Thus, regulatory work is no longer carried out by centralized institutions (especially not by exchanges themselves), but by every participant in the distributed network who has equal regulatory authority. Just as every user can trace the source and flow of funds of every blockchain wallet address on the blockchain network, every user should also be able to regulate the exchange they use, provide timely evidence and report improper behavior when it occurs. This is the concept of decentralized regulation that we advocate for (Figure 2).

Figure 2

Decentralized supervise = Everyone （Users, governments or businesses ） can be supervisor

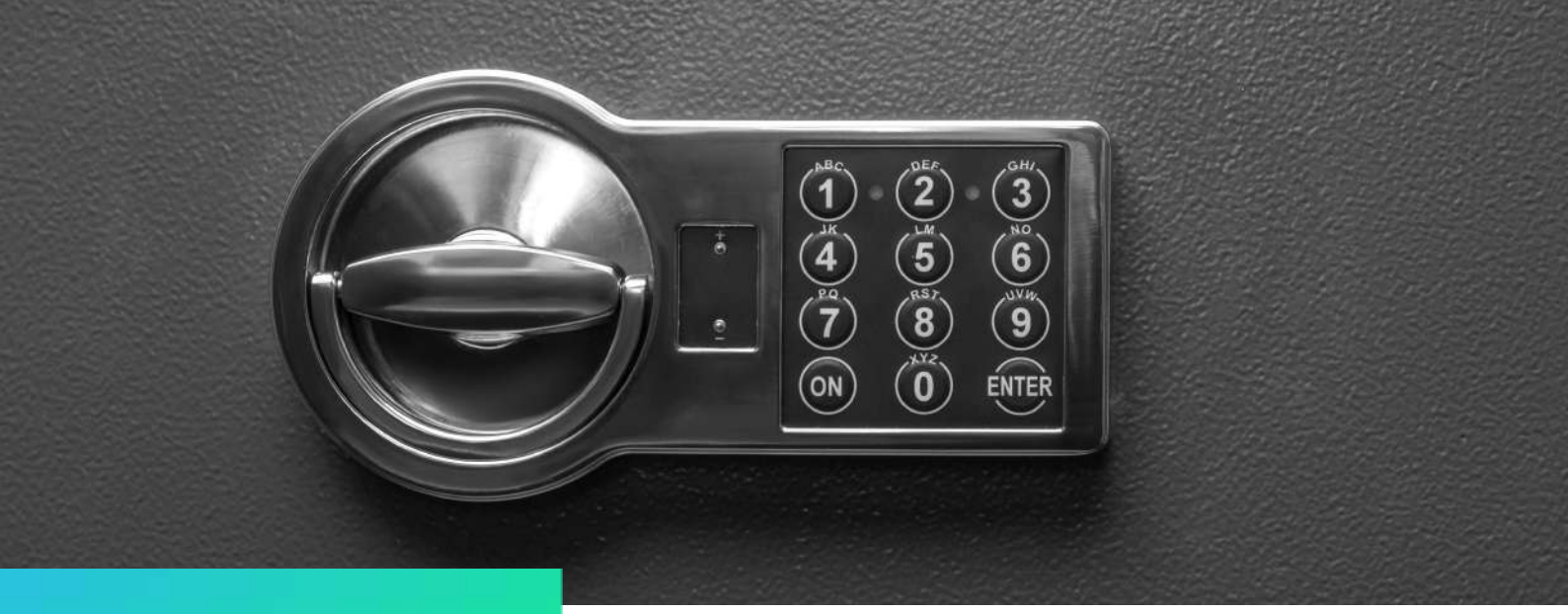


AIT Government

With the rise of emerging technologies and changes in regulatory environments, business models and customer experiences are constantly evolving and innovating. Risk management issues faced by the development of financial technology, including strategic risk, operational risk, network security and data risk, and operational and financial risk, among other aspects, will become more complex, diverse, and challenging. Therefore, risk governance of financial institutions in the digital financial era will move from single-point management towards integrated value chain ecosystem governance. The use of regulatory technology, or RegTech, is a way to strengthen risk management. For example, the deployment of a data risk analysis platform application blueprint for enterprises, targeting internal (information security, data protection, internal control loop) and external (competitor information, partner data, and open data) areas, can progress from single-domain deep analysis to comprehensive analysis across domains. At the same time, effective abnormal access rules (people, things, time, place, and objects) are established, and through a network threat intelligence analysis platform, external threat information is automatically collected, internal information is integrated, and security trends and risk analysis reports are generated. Active management is carried out based on the audit trail, giving data applications a new perspective and enhancing the role of data analysis in risk management.

03

Decentralized Identification and Asset Protection



TideBit Connect

TideBit Connect is an open identity verification standard that has gained support from many large enterprises and organizations. It provides a more secure and convenient way of identity verification. Using public-private key electronic signature and verification technology, all users can create and keep their own private keys, sign in to any system, and authorize various operations through their private keys, greatly enhancing security.

TideBit Connect is a standardized technology that supports multiple platforms and devices. It can be used with hot wallet software such as Metamask, imToken, Trust, and other apps, as well as multiple cold wallets including Ledger, CoolWallet, AT Wallet, and other hardware wallets, providing users with more options to store their decentralized identities.

Overall, TideBit Connect's identity verification technology has higher security, better user experience, standardization, and cross-platform advantages, aiming to become the technology standard in the field of identity verification.

TideBit Vault

TideBit Vault is a blockchain asset safekeeping technology that generates a unique TideBit Vault for each TideBit Connect identity to securely store the user's blockchain assets. Unlike traditional centralized exchange technology, when a user deposits blockchain assets to TideBit, TideBit creates a separate TideBit Vault for each user to safeguard their assets.

TideBit Vault uses Partial Private-Key Protection (P3) technology developed in-house, where asset usage requires designated private key signature and platform verification before a blockchain transaction can be executed to transfer the designated asset. This ensures that the exchange cannot use the user's assets, and even if malicious hackers invade the exchange, they cannot compromise user asset security.

In addition, TideBit Vault analyzes the risk of user theft and illegal activity. When the system determines that a user may be subject to theft or illegal activity, it can immediately interrupt the operation to prevent user losses.

KYC over Blockchain

When a user undergoes identity verification through TideBit Connect technology, we identify the private key as a unique individual customer, but legally the user remains anonymous. To maintain the safety and security of customers and their assets, TideBit uses multiple risk control technologies to ensure the fairness and security of the trading market and to prevent money laundering or the financing of terrorist activities on the exchange. One of the methods used is blockchain customer due diligence.

TideBit asks and verifies users to provide locally government-compliant natural person or legal entity identification documents. After confirming that the documents belong to the user, TideBit guarantees that the private key can represent the customer to execute all locally government-regulated behaviors. In addition, TideBit, with the user's consent, investigates the legality and credibility of the user at the identity verification agency, while comparing high-risk crime lists provided by international organizations to execute corresponding measures according to the customer's risk level.

Blockchain Assets Tracker

In order to maintain the moral order of the financial society and effectively curb financial crimes, TideBit has independently developed the Blockchain Assets Source Tracker (BAST) to analyze the source of every blockchain asset deposited to TideBit, and to compare the possibility of whether the asset is derived from financial crimes with international crime analysis. In addition to source analysis, we also analyze the correlation between the asset source address, asset withdrawal address, and high-risk crime lists, and can determine the user's risk level within one hour and complete local government notifications and temporary asset freezes within 24 hours as contingency measures.

04

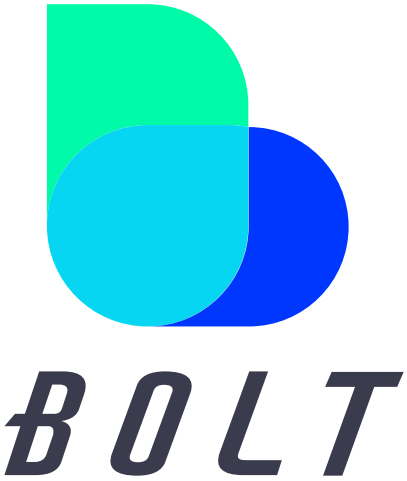
Decentralized Regulation

BOLT

Decentralized Regulation Technology

Since 2016, TideBit has been discussing the blockchain technology and Fintech ecosystem with financial institutions from various countries, including the Hong Kong Stock Exchange (HKEX). According to the needs identified, TideBit has designed its own decentralized regulatory blockchain technology, Blockchain Open Ledger Technology (BOLT), which is used to implement accounting, auditing, and certification requirements for various financial technology systems, including TideBit Exchange. This technology has also enabled a Taiwan technology company to obtain a financial license for securities trading under government guidance.

BOLT is an open and decentralized ledger technology that anyone can download and run as a blockchain node to maintain its operation. In terms of technical design, BOLT ensures that data cannot be tampered with on the blockchain, and uses zero-knowledge proof technology to allow data stored on the blockchain to be inspected and investigated by third-party audit units without the risk of confidential information leakage.



From 2018 to 2019, BOLT collaborated with the Hong Kong Stock Exchange (HKEX) to develop a series of blockchain technology applications for auditing, including:

Proof of Reserve for Financial Institutions

Converting financial products such as stocks, funds, and bonds into blockchain assets and recording their transaction history in full based on smart contracts.

Enterprise internal control / regulatory compliance

Implementing enterprise artificial intelligence digital governance on the blockchain, with all enterprise accounts stored on the chain through zero-knowledge proof technology to prevent illegal activities.

Big data application/anti-counterfeiting traceability

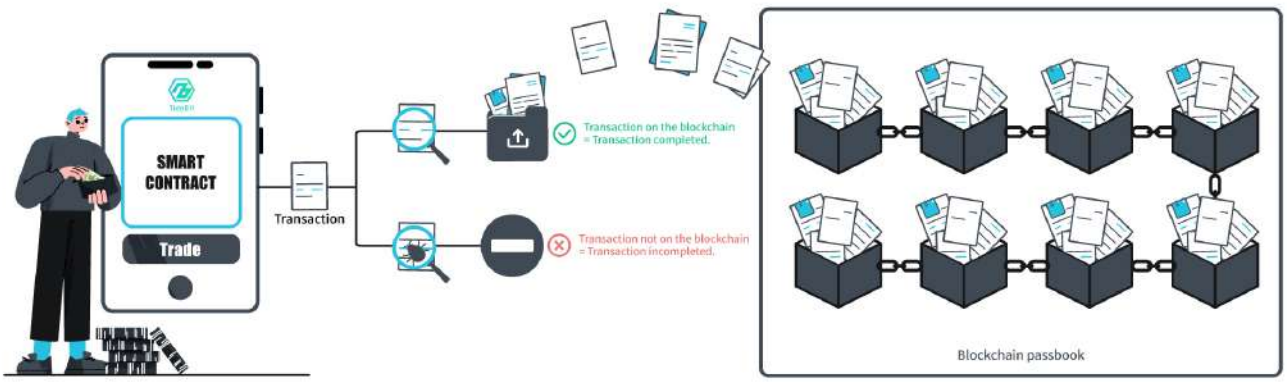
Providing blockchain-based solutions for product logistics and supply chain management, and offering a unique identity authentication mechanism for each product to defend against counterfeiting and provide users with a complete product history.

Real-Time Evidence and Audit

All user actions on TideBit, including depositing or withdrawing blockchain assets, executing or canceling spot trades, are done using smart contracts running on BOLT. Therefore, all transaction records will be stored on the blockchain. Each user's order request will be fairly processed by the smart contract on the blockchain, replacing the agent mechanism with an algorithm, achieving absolute fairness, openness and transparency. Users can also confirm this on the blockchain browser and obtain relevant evidence.

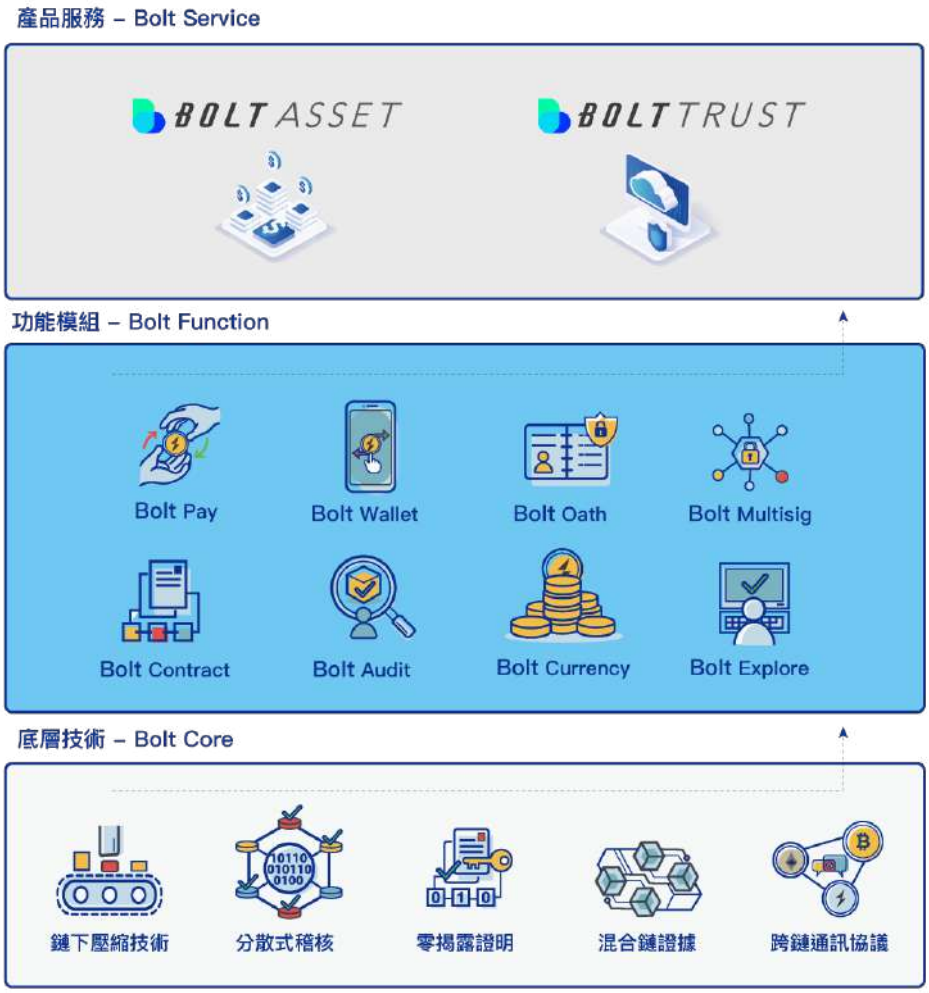
Different from traditional accounting and auditing mechanisms, all transactions on TideBit exchange are real-time records, and the evidence of all transactions can be publicly available on the blockchain as soon as they are established. At the same time, all transactions are delivered to all blockchain nodes at the moment of their creation (as shown in Figure 3), and are audited in real-time according to the specifications on the smart contract using algorithms instead of manual auditing. This not only eliminates the limitations of traditional accounting and auditing cycles, but also creates the most fair and transparent contract execution platform. Any transaction that violates the user's intention or the smart contract terms will be immediately rejected by the blockchain after the evidence is submitted.

Figure 3



Real-Time Audit

Figure 4



BOLT Architecture

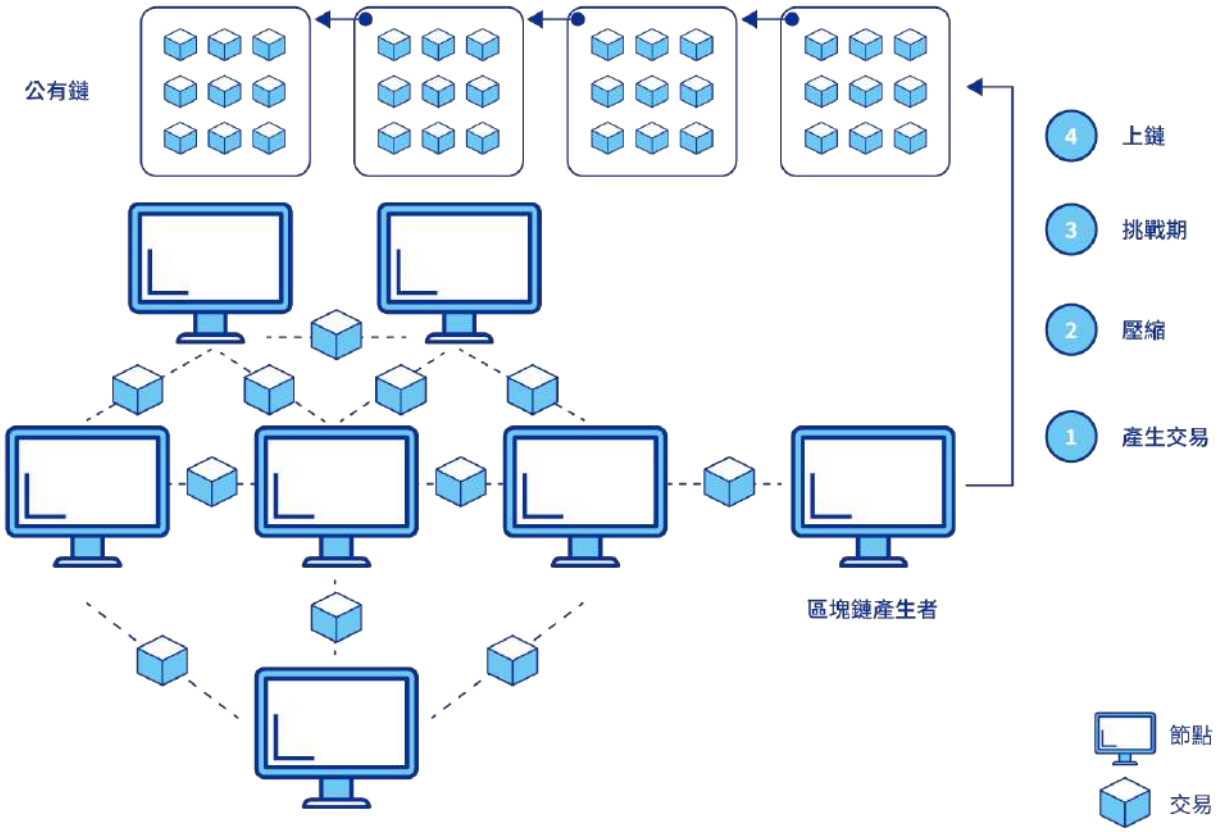
Efficient Coordination Protocol

BOLT uses a special communication protocol called Locutus, and nodes regularly define a communication tree network called Borg–Tree based on consensus, where all nodes can connect to each other. In this network, information sent from any node will have the fastest delivery mode and quickly spread to all nodes.

Serialized Secret Certification

To achieve global consensus, BOLT is designed to collaborate between unfamiliar nodes without the need for centralized server control. Its operating protocol is published through smart contracts on the blockchain. Participants in BOLT obtain the protocol and follow the published guidelines (Figure 5).

Figure 5



Serialized Secret Certification

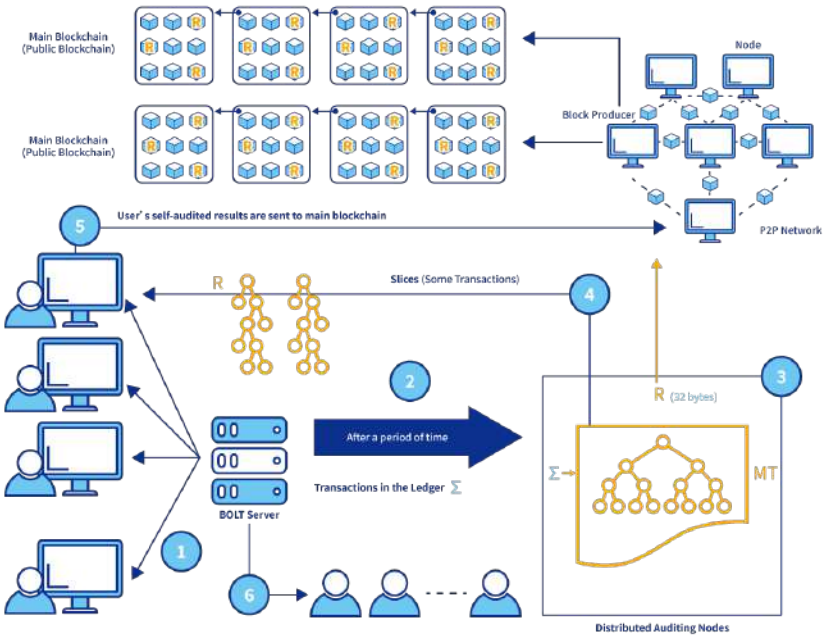
Cross-Chain Channel

BOLT's cross-chain blockchain architecture is shown in Figure 6. Cross-chain refers to a collaborative operating mode composed of multiple parallel blockchains (Paralle Blockchain). For general blockchain transactions, such as cryptocurrency transactions or single contract records, users will directly send transaction information to the P2P network of the blockchain, and finally fixed on the main chain by the node that becomes the block producer. These transactions are limited by the characteristics of the blockchain, which may result in higher transaction costs and slower transaction speeds. Therefore, when a large number of high-speed transactions are required, transactions can be sent to BOLT for execution. BOLT's operation is high-speed, and after accumulating a large number of transactions over a period of time, the hash value and related identifiers are generated by the decentralized audit nodes of the system and sent to nodes through cross-chain protocols to be fixed on other public chains. The entire cross-chain blockchain architecture of BOLT consists of "ordinary nodes" (hereinafter referred to as nodes) and "audit nodes" to form a decentralized operation of the entire system.

BOLT adopts a hierarchical architecture to achieve consensus among the main chain at the top level, while the validity of transactions for each application is achieved by the data structure of lower level side chains (which can be composed of any data structure), which can be generated at any time and without limitation. This makes it ideal for solving the problem of interfacing real-world scenarios with blockchain. In addition to increasing bandwidth and solving problems related to large amounts of data and privacy protection on the chain, BOLT's features also address the difficulty of integrating current application systems with decentralized systems.

In BOLT's multi-chain operation, the consensus of the main chain is achieved through the global consensus of public chains, while the validity of the side chains and how to maintain correctness and avoid single point of failure or malicious attacks by agents (or audit nodes) are achieved through BOLT's designed side chain operation, including decentralized audit functions.

Figure 6



The transaction evidence on BOLT needs to be packaged into a block at regular intervals and broadcasted to all nodes to form a consensus. Due to the use of Hybrid Consensus Evidence (HCE) to ensure its tamper-proof characteristics, the consensus among nodes in BOLT requires more complex division of labor and processing than other blockchains. All nodes that participate in the entire BOLT consensus process can receive corresponding rewards based on their level of contribution. The following lists the node roles and responsibilities in the BOLT consensus mechanism, and each node can perform multiple roles.

Cluster Manager

Responsibilities of this role are maintaining the node member list, regularly scoring members and maintaining member reputation information, and broadcasting and coordinating information. All communication behavior of the consensus mechanism is delegated by this role, while also ensuring that a node's reputation must reach a certain level before executing a specific role. BOLT uses an improved Raft algorithm to manage the cluster and uses its unique broadcast algorithm technology, Locutus ensure all consensus can be completed in the shortest time with a consistent node list.

Block Packager

The responsibility of this role is to verify existing transactions, package them, and generate compressed evidence based on the aforementioned technology. Nodes confirm that each other's data is correct based on the evidence, thus completing the packaged consensus. They then continue to generate cross-chain evidence, encrypt the packaged transactions, and upload them to IPFS for storage.

Auditor

This role requires conducting a quick data inspection after the block packager completes their work. Nodes will determine their audit scope within the block based on an algorithm, allowing them to quickly verify the correctness of the evidence before it is uploaded to other blockchains, and then generate an audit consensus. This consensus link requires a complex mechanism to ensure its immediacy, and detailed information will be supplemented in the next chapter.

Coordinator

Nodes in this role are responsible for different blockchains, and after achieving the audit consensus, they upload the completed cross-chain evidence to the blockchain they are responsible for, while also incurring the cost of uploading. Through these consensus mechanisms, BOLT can ensure greater protection against attackers, and the addition of new nodes only requires requesting BOLT data from other blockchains and IPFS, greatly improving the overall security of the system.

Distributed Auditing

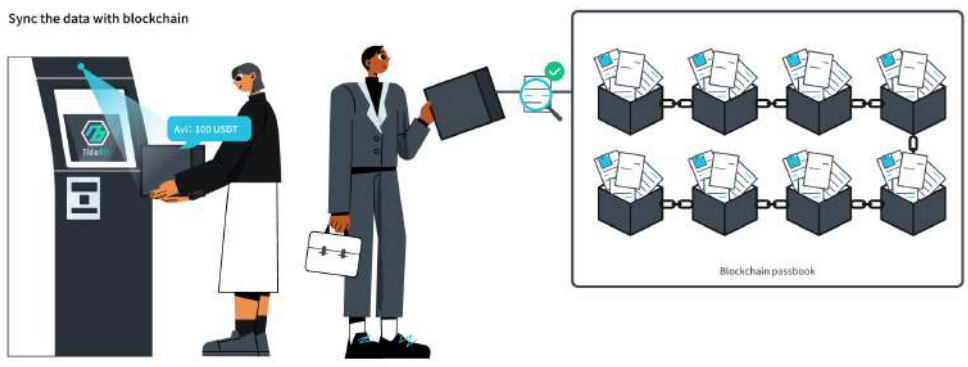
With PoHCE consensus mechanism, verifying blocks and transaction data becomes more complex, involving interactions with smart contracts on other blockchains. This leads to a significant increase in time costs. Therefore, we need a mechanism to divide the auditing tasks and ensure that they do not affect system performance.

In a decentralized system with agents involved, the main problem is whether the agents will record the correct transaction on the blockchain. BOLT's decentralized auditing technology can solve this problem. Because the operation of the sidechain agents is still audited through decentralized means, the entire system still maintains the concept of decentralization. Some systems were proposed during the early development of Bitcoin that allowed agents to process some transactions before recording them on the blockchain, but these systems could not solve the problem of black-box operations by agents, which goes against the concept of decentralization in blockchain and therefore could not be widely accepted.

In sidechain, all transactions are stored in the indexed Merkle tree and its root hash value is publicly announced. After that, a participant or a provider of digital assets can locate a certain transaction in the bottom layer node of the indexed Merkle tree immediately through the index function. To audit their own transactions or verify whether they exist in the transaction ledger, participants can request the agent to audit a certain transaction. Since the participant has the transaction's sequence number (the completion of this transaction has the agent's digital signature, so the agent cannot deny it), the agent must present the slice of the transaction. Consumers can use the root hash value of this ledger and the slice of the transaction to verify whether the transaction is correct or exists in the transaction ledger.

Decentralized auditing build-up the blockchain ecosystem, not only do block producers have arbitration capabilities, but they also receive rewards based on their block production and verification contributions.

Figure 7



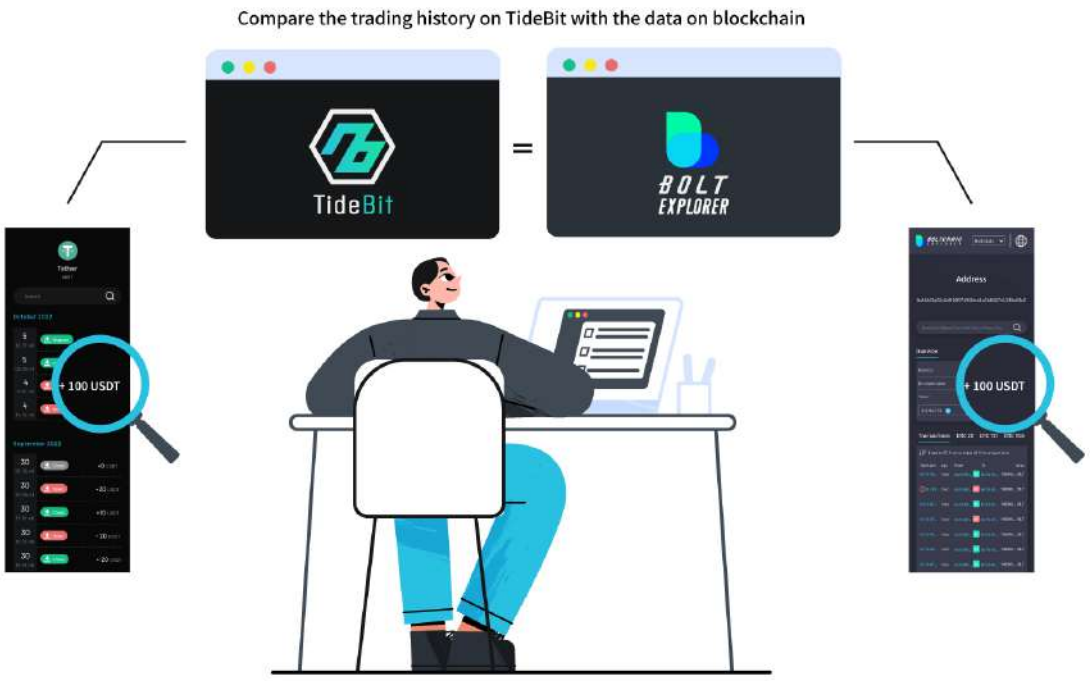
uneditable ledger

User Self-Auditing

To ensure user privacy, transaction details are stored on the blockchain in encrypted BOLT Evidence format. TideBit users can download their own transaction data in plaintext from TideBit in any situation; even if the TideBit exchange is damaged or discontinued, users can download BOLT Evidence from the blockchain that records all their transaction history. Users' plaintext transaction data is not only permanently stored on TideBit, but users can also save it themselves. With sufficient blockchain knowledge, users can independently audit all content (Figure 8). These transaction records contain electronic signature evidence recognized in the laws of multiple governments, allowing users to verify at any time that there is no transaction behavior on TideBit that violates their wishes.

In addition to self-regulation and self-audit, users can also submit relevant evidence to other third-party blockchain companies for audit investigations.

Figure 8



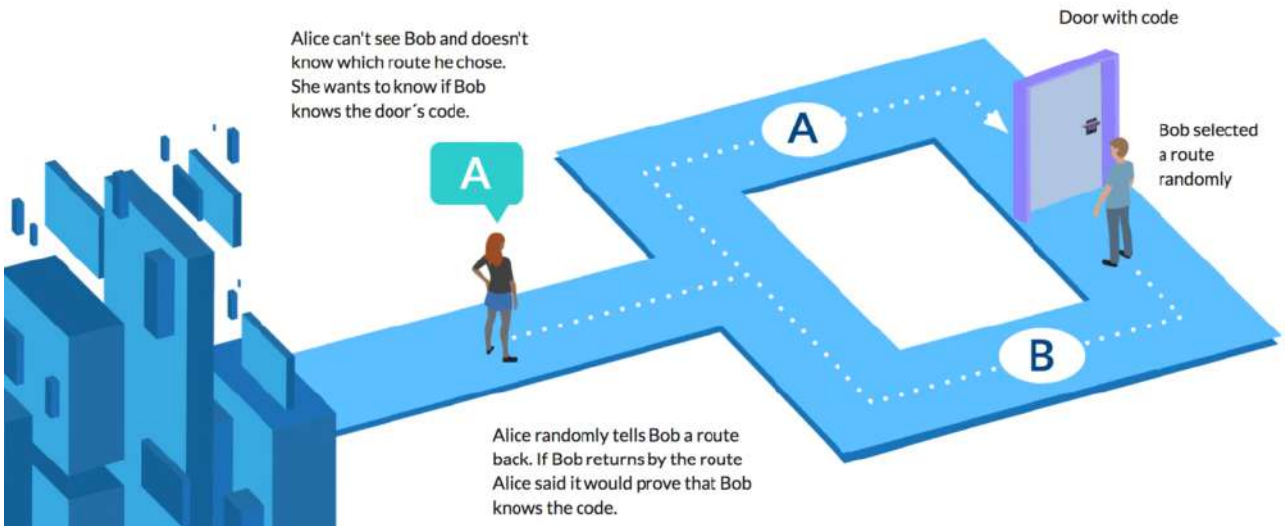
User Self-Auditing

Zero-Knowledge Auditing

To ensure user privacy, transaction details are stored on the blockchain in encrypted form using the BOLT Evidence format. TideBit users can download their own transaction data in plaintext from TideBit at any time, even if the TideBit exchange is damaged or stops operating. Users can also save their own transaction data and independently audit it if they have sufficient knowledge of the blockchain. These transaction records contain electronic signature evidence recognized by multiple national government laws, enabling users to verify that no transactions on TideBit violate their will.

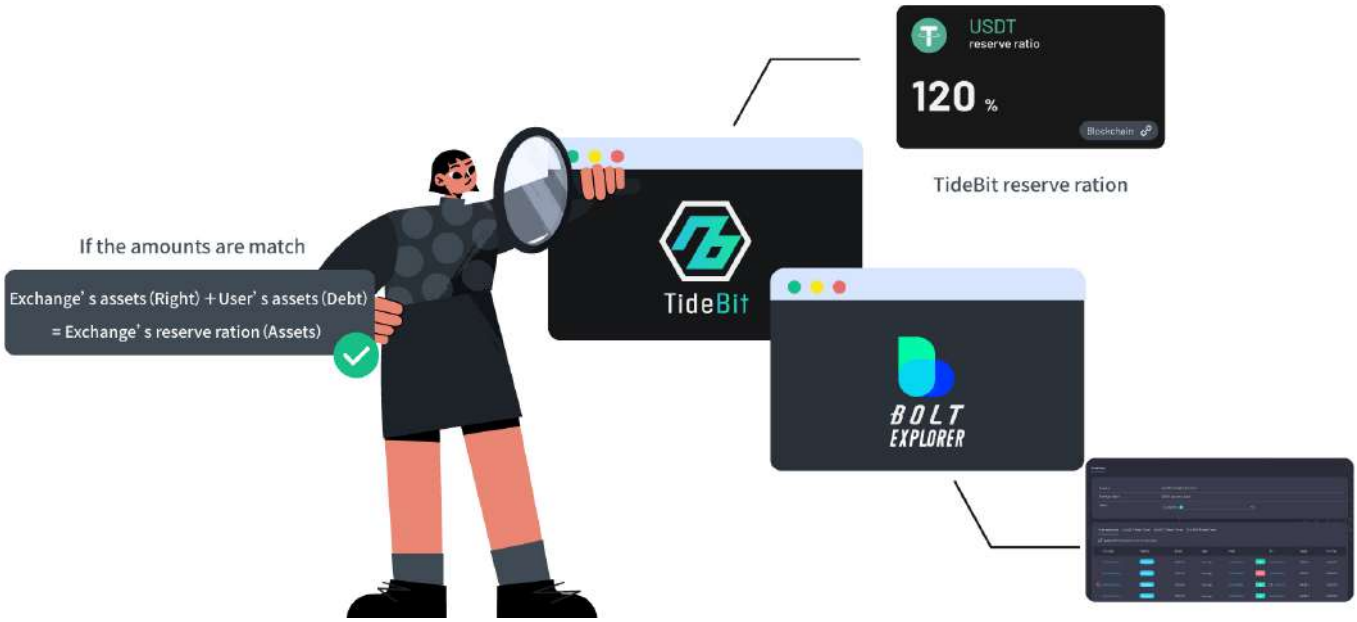
In addition to self-regulation and self-audit, users can also submit relevant evidence to other third-party blockchain companies for audit and investigation. To ensure user privacy, each piece of transaction data is transformed into a special BOLT Evidence format that can be easily computed and verified using mathematical foundations. All unencrypted transaction data for every transaction is permanently stored within TideBit, and in specific cases, third-party audit units may require decrypted actual transaction data to investigate events in full. TideBit has designed the most comprehensive custodial responsibility handling process policy, and third-party units can obtain plaintext data from the blockchain by holding user private keys to sign the agreed smart contract, or by providing relevant legal documents authorized by the user's local government to TideBit for plaintext data.

Figure 9



Zero-Knowledge Proof

Figure 10



Proof of Net Reserve

Proof of Net Reserve

As an open financial technology service platform, TideBit ensures the safety and transparency of its operations with the most advanced technology. TideBit provides academic and technical standards for auditing and verification, and adheres to risk management processes that exceed industry standards. All user funds are stored in TideBit Vault, and we continuously record all asset flows in TideBit Vault around the clock, which are promptly disclosed on TideBit. Through this public information, users can independently verify the credibility of data on the blockchain, ensuring that TideBit always has sufficient blockchain asset reserves.

Market Aggregation Engine

As of 2022, there are over a thousand centralized or decentralized blockchain asset exchanges around the world, leading to increasing market fragmentation. Since these exchanges cannot share liquidity with each other, there is a huge disparity in market conditions, resulting in reduced trading efficiency and significantly increased user trading costs under such market barriers.

TideBit has developed its own liquidity aggregation engine based on the BOLT blockchain, which integrates market information from different exchanges and provides users with real-time access to the best trading strategies between exchanges on TideBit.

Zero-Domain Order Engine

The trading orders executed by users on TideBit can not only be executed on TideBit but also be instantly mapped to other serviceable exchanges, ensuring users' rights and interests are not affected in any disaster. As TideBit operates on BOLT blockchain technology, as long as there are normally functioning BOLT nodes in the market, users can continue to use TideBit services. Users can still freely withdraw their blockchain assets stored on TideBit, and continue to execute transactions on other exchanges.

Zero-Domain Trading Engine

Through our Real-Time cross-domain order aggregation system, we have developed a cross-domain trade matching engine based on blockchain smart contract auditing technology on TideBit. This allows users to execute cross-domain matches across different exchanges, greatly improving the efficiency of blockchain asset trading.

05

Conclusion

Since 2017, TideBit has received guidance from a large number of financial institutions, especially the Hong Kong Stock Exchange and the Financial Supervisory Commission of Taiwan, and has accumulated a great deal of practical experience. We have been continuously committed to the research and improvement of blockchain technology, hoping to bring new and positive impact to the world in the field of financial technology. For this reason, we have designed the TideBit 2.0 update plan that incorporates our past experience, and at the same time, we are announcing the BOLT blockchain technology that our team has been developing for years. We hope that in the future, while we continue to improve TideBit, we can also promote the improvement and progress of financial services, and facilitate the development of human society.

TideBit