

ABSTRACT

Data chain is a block-chain technology integrated application platform, with tree-like layered, three-dimensional architecture, while adding regional chain technology 2.0 as the core of the intelligent contract platform, distributed application of the underlying protocol and other innovative technologies .DTC(Data-Chain) will focus on the data storage, analysis and decision-making of various industries, while working with other application chain to achieve DTC transactions in various types of data and circulation in the future to become the industry data applications .

With the second-generation block-chain technology, such as Ripple, Ethereum and so on, the two-generation technology pushed the block chain to the regional chain 1.0, Application development stage. So that more and more regional chain applications began to flow in the city, resulting in rapid growth in the regional chain of data. DTC can link an application through the side chain, and provide a number of data analysis, the data classification. DTC can handle multiple applications in parallel because of its side chain functions or through intelligent contractual means. The unique non-modifiable records of the block chain can show all the data trajectories of the enterprise application during operation, greatly improving the product's advantages in traceability.

DTC's goal is not only in the application of data processing for the regional chain, in our development strategy, DTC will become the regional chain of circulation media, that is, the regional chain "bit currency." To this end, DTC R & D and community hope that with the like-minded friends together for the development of DTC continue to forge ahead.

Unlike nearly all other decentralized exchange platforms, this allows for decentralized exchange of other blockchains and between multiple blockchains directly without a trusted gateway token. Markets may be able to significantly reduce spreads and encourage market assurance via decentralizing custody and increased transparency of market activity. This is achieved using smart contracts, protocol tokens enforcing correct market behavior of orderbook matching, a new construction of Ethereum

bonded external enforcement of clearinghouse activity, and commitments to historical exchange data for use with Ethereum smart contracts

Catalog

Chapter One Blockchain Development.....	1
Chapter Two DTC.....	2
2.1 Design Background.....	2
2.2 DTC Technology.....	4
2.1.1 Merge Mining.....	4
2.1.2 Token Model.....	5
2.1.3 Sidechain.....	5
Chapter Three Feature.....	7
Chapter Four Application.....	8
3.1 Data Interaction.....	8
3.2 Social Governance.....	9
3.3 Decision-tree Application.....	9
Chapter FIVE Conclusion.....	10

Chapter One Blockchain Development



The concept of the block chain inherited the bitcoin, which is what we often say in the regional chain technology 1.0. The concept of Bitcoin was originally proposed by Nakamoto in 2009, according to the idea of the open source of the open source software, Bitcoin is a P2P form of digital currency and its core ideas - point to point transmission. It means that Bitcoin is a decentralized payment system, with the main characteristics.

Bitcoin is the difference between the majority of the currency, the currency does not rely on specific currency institutions issued, it is based on specific algorithms, through a large number of calculations, the total number is very limited, with a strong scarcity. Bit currency economy uses the distributed database of many nodes in the entire P2P network to confirm and record all the transaction behavior, and use the cryptographic design to ensure the security of all aspects of currency circulation. P2P's de-centricity and the algorithm itself can ensure that the currency can not be manipulated by a large number of manufacturing bits. A cryptographic-based design allows a bitcoin to be transferred or paid only by the real owner. This also ensures that the ownership of money and the anonymity of circulation transactions.

And now because of the community and technology to promote, we ushered in the regional chain technology 2.0. One of the representatives is the ether square. Ethernet Square is a chain in the chain to achieve intelligent contract, open source of the underlying system, the ether from the birth of the week to 2017 May, just three and a half years, the world has more than 200 application of the application of the tower. Ethernet is not only a platform, it is a programming language, so that developers can build and publish the next generation of distributed applications. The etherbox can be used to program, publish, and so on, such as voting, domain names, intellectual property, and traditional industries such as agricultural records.

Chapter Two DTC

2.1 Design Background

The Ethereum is created by the creation of digital assets, but its Turing complete virtual machine system also provides more imagination, bringing people from the field of digital assets to many other areas. The concept of block chain fire up the reason, but also because we put the bottom of the digital assets of the chain of technology and digital assets itself peeling off, began to discuss the application of the upper layer began to fire up. We know that the block chain is just a bottom of the operating system, a chain of value transmission. On this basis, we can build countless business applications we want, everything and "buy" or "sell" the relationship between the application, can be built in such a block chain, the ether square is actually such a system. It extends the bit-chain concept of Bitcoin: verifies, stores, and replicates transaction data on multiple computers worldwide. The Ethereum goes further on this concept, making it possible to run code on multiple computers around the world. The tomb of the ether is called ether (Ether), or ETH. Similar to BTC, this encrypted currency can be used to trade with other encrypted currencies or other currencies.

In short, Ethereum is an innovation that applies some of the techniques and concepts in Bitcoels to computing. Bitcoin is considered a system that maintains a shared book that safely records all bit currency bills. The Etherhouse uses a number of mechanisms similar to Bitcoels (such as block-chain technology and P2P networks) to maintain a shared computing platform that can be flexible and secure to run any program that users want (and, of course, similar bits Currency block chain program). Block chain technology is considered to be the most disruptive technological innovation

since the invention of the Internet. It relies on cryptography and Hash function, game theory and so on. It can not build trust on the Internet without any third party.

Intervention can make the participants reach a consensus, at a very low cost to solve the trust and value of the reliable delivery problems. Since the bitcoin, many block chain projects have sprung up, many of which have groundbreaking innovations, or innovation at the bottom of the agreement, or innovation at the application level. These blocks are available from the industry Experimental significance.

The primary role of blockchains are to solve coordination problems among multilateral agreements between a network of participants. By ensuring transparency, assurance, and enforcement, we can enable multilateral agreements where they were not previously possible. When all parties are assured that the operations are not only transparent, but also the mechanisms are guaranteed to not change without significant effort, parties are more willing to coordinate. Participants have significantly higher guarantees that a single party has difficulty forcing other parties in the future into usurious rent extraction via a change in business processes or information asymmetry. In other words, any single participant is more willing to use systems where the business processes and mechanisms itself are not owned by any other single participant. There is a fundamental coordination problem amongst payment processors, gateways, and financial institutions. For instance, a customer of a bank wishes to pay a merchant on another network. Traditionally, there have been significant efforts in engineering around payment systems which are compatible across payment networks and financial institutions. These are usually constructed by creating a clearinghouse which manages the interchange, usually via a messaging network with either a central counterparty clearinghouse or nostro/vostro accounts. Examples include FedWire, CHIPS, SWIFT, consumer card payment networks, NSCC/DTCC, OCC, and ACH. These networks service different roles and functions, including local/national payments, international payments, credit, equities/asset exchange, and derivatives. These centralized networks allow for the controlling entity to arbitrarily change the mechanisms, which result in significant amount of transaction costs via information costs, due diligence, and contractual enforcement between all parties.

DTC is in this context, as before the Internet applications, when the application has sprung up, we believe that the final core is still the data acquisition and understanding. Only to win the data in order to obtain to the user, in order to achieve the value of the

application. The DTC is such a vision, is willing to become a regional chain in the application of data flow, in this wave of technology to win their own place.

2.2 DTC Technology

Merge Mining

We have been very clear mining is the beginning of the CPU mining, excessive GPU mining, and ultimately evolved to the current era of ASIC mining. The evolution of mining is the evolution of hardware, but also the evolution of software, especially the hardware and software docking protocol improvement process. The DTC decides to use the POW + POS hybrid consensus mechanism, both of which have equal weights, and the POW and POS blocks in the block chain are designed to be 1: 1. Before the existence of the POW consensus because the proportion of design is too large, resulting in the late mining area of the POS block no one to dig. The DTC team felt that POS + POW should coexist and increase the ecological stability of the DTC mine. The difficulty of these two mechanisms will be constrained to each other, and with the same type of continuous block increases, the difficulty will be an additional increase. This hybrid approach does not weaken the security of any single consensus mechanism. The security of the block chain fully combines the advantages of POW and POS, and the attack on the block chain will become more complicated. On the one hand, due to the existence of POW, Who also need a large number of coins to achieve double payment attack. POW costly, energy consumption, but the system is relatively strong, POS is not a waste of energy, but its safety performance has not yet been recognized, and fairness there are some controversy.

Token Model

An asset issuing entity sends a transaction in the Bitcoin network with a "asset founding" metadata that actually amounts to creating a token that is used to represent an asset. The ownership of these tokens on the bit network, without the need for asset issuer authorization, you can freely flow of transactions. In fact, a token is an asset of

the digital, bearer bonds, but this bond is embedded in the assets of the unit coin in the block chain network. In the tokens model, there are two main types, UTXO model and Account model (account model), bit currency and derived block chain system are using UTXO model. But now only the contract is also more and more used in tokens. Intuitive, Account model is more in line with people's daily habits, in most cases, people only care about how much income, how much expenditure, the balance of how much, regardless of the specific consumption of which income. After a comprehensive consideration, DTC uses UTXO mode, you can in a fixed account has been stored DTC token.

As DTC requires fullnode validation of the public Ethereum blockchain for maximum efficiency and security, it's possible to create a contract on the Ethereum blockchain which locks up funds dependent upon the condition of the DTC chain. These funds are now bonded and locked and its activity is enforced by the DTC chain. When an order executes, a proof is provided to unlock the funds on the Ethereum side. This construction presumes that Schnorr or BLS signatures will be available on Ethereum in the near future. A transaction tracks the activity of the DTC chain, and needs some level of maturity confirmations before payment is delivered on the Ethereum chain. Funds can still be settled on DTC and balances updated for continued trading, it is only for final delivery when the payment occurs on Ethereum. The behavior of the DTC chain enforces the behavior of payments on the Ethereum chain. In an non-adversarial environment, a Lightning-like construction is available where a user can provide a payment directly without proof, and if the payment is not disputed after a certain amount of block maturity, is paid out without needing blockchain proof/computation. In the event the payment does not match the state in the DTC chain, anyone can provide proof and the sender's balance would be slashed. This allows for greater computational and bandwidth efficiency on the Ethereum chain. This construction on the DTC chain is for trading Ethereum, Ethereum-like chains, and Ethereum issued tokens similar to ERC-20 using bonded smart contracts.

Sidechain

The side chain is a special block chain. It uses a technique called "SPV wedge" to achieve asset transfer with other block chains, which allows users to use the existing

assets to use the new encrypted money system. People do not have to worry about Bitcoin difficult to adopt innovation and adapt to new needs, as long as the creation of a side chain, and then docked to the bitcoin block chain can be inherited and reuse Bitcoin strong block chain, but also to avoid the new Currency liquidity shortages and market volatility and other issues. And because the side chain is an independent, isolated system, serious problems in the side chain only affect the side chain itself, which greatly reduces the risk and cost of innovation. The flexibility of the side chain is also reflected in the fact that all the block chain parameters can be customized, such as block spacing, block rewards, transaction fees, etc., advanced users can also modify the consensus algorithm. But the most important thing is the business logic, the side chain can be easily developed with your business-related transaction type or smart contract. This is different from the inventor blockstreams of the side chains, the side chains of the blockstreams are just a different currency system, and it is not easy to develop new deals and smart contracts.

This network is an open network, it is necessary for accurate trading activity to require activity on the decentralized exchange to eventually be public, even with blinded commitments/bids. While new cryptography is possible via SNARKS, it is currently too slow and resource intensive for a high-volume trading network. We are currently optimizing for performance and speed. Since this is a pseudonymous network natively (with optional AML/KYC constructions for issued tokens). SPV validation of other chains is presumed to be insecure with blockchains that do not discourage reorganizations. For chains which allow reorgs, either full-node validation of that chain is required or an HTLC-clearinghouse construction is needed. It presumes that Ethereum will create greater reliability and guarantees around finality (current Proof-of-Stake research). These technologies are new and not yet tested. While we will do our best to construct it with maximum security in an adversarial setting, we are modeling the security model of these mechanisms which require real-world use case with human behavior to properly understand. When interaction between chains, it is difficult to roll-back errors, one should only put the minimum necessary to transact at a time on this chain when doing significant decentralized cross-blockchain activities. Initial versions may have less robustness in adversarial settings, and we recommend lower values at stake, as often times attacks (especially Denial of Service attacks) are resolved over

time as the software develops. Performance and real-world behavior implications of the design is not yet clear

Chapter three Feature

The above mechanisms require significant volume of activity (with a large amount of state), and is not at this time suitable for all activity to occur on the Ethereum main chain, however the construction would be to bond trading activity in the public Ethereum chain with contract execution input being provided by the data-chain. We are building a blockchain which hooks into other blockchains to allow for trading across token/asset classes, largely backed by Ether. From the perspective of any individual chain, we are building a scalable blockchain whose contract state is bonded by the activities of the data-chain itself. Activity on other chains can interlink with this chain via interchain committed proofs similar to BTC Relay on the data-chain which can be submitted on Ethereum. The data-chain validates the activity of the behavior of all participants (including activity on other chains). In other words, the role of the data-chain token is providing computation and enforcement. The token itself acts as a bond for its activity on this blockchain, improper activity results in the token/bond being burned on the data-chain. By creating a custom chain with deep enforcement, we are able to construct a system where consensus rules optimize for high-performant activity. The design optimizes for rapid execution and clearing, with slower settlement. Future iterations may include sharding of the data-chain, but the initial iteration will presume high-throughput capacity for block propagation. Owning data-chain tokens buys the right to validate this blockchain, within its consensus rules. Transaction fees on the network including (but not limited to) payment, interchange, trading, and clearinghouse use, are given to non-faulty validators who enforce bonded contract states. The token will have value derived from the fees derived from this network, with the obligation/cost of providing validation to its users. This token must have value, to prevent low-cost attacks and is necessary to enforce this network. It may be on our roadmap to allow for delegating validation to third-parties, whereby a limited amount can be slashed at a time before re-delegation is required (the exact mechanism is not yet specified for security modeling). As this will be designed as a high-performant system,

an linked-via-proof blockchain construction is necessary. We expect that this system will be able to handle extremely high volumes of transactions and hence, will only do final delivery over Ethereum. Clearing and settlement occurs over the data-chain blockchain. Consensus rules are enforced via this proof-of-stake network. As part of the consensus rules of this network, it is required that all data-chain validators also run the Ethereum network to validate in parallel, resulting in Ethereum as a first-class citizen with regards to inter-blockchain validation. It is assumed for features such as Ethereum/ERC-20 bonding and withdrawals that BLS signature schemes (or alternatively Schnorr) will be enabled in Ethereum in the near future. For cryptocurrencies, these tokens are non-custodial and instead locked in smart contracts (unlike other exchange platforms such as Ripple, which requires trusted gateways representing the underlying). It also does not rely on named centralized validation sets (e.g. Ripple). The data-chain manages matching and managing order execution on the Ethereum chain. Activity on the data-chain ensures the validator activity also may be enforced on the Ethereum chain via native Ethereum smart contracts. For Bitcoin and Bitcoin-like systems, we allow for trading via a clearinghouse network on the Lightning Network. The blockchain enforces activity on this network via committed proofs. While not as robust as Ethereum's network, it allows for near-instantaneous clearing and settlement of activity orchestrated on the data-chain without full-node validation. We expect to do partial validation in the future for nodes which do not allow for blockchain reorgs; naive SPV validation with blockchains that support reorgs are not permitted on this network for security.

Chapter Four Application

2.1 Data Interaction

DTC can be used for enterprise data decision-making, for the global small and medium enterprises to provide data sorting, analysis and decision-making. DTC can link an application through the side chain, and provide a number of data analysis, the data classification. In the process of data analysis, through the depth of data mining analysis, you can form a user portrait, will bring a threat to personal privacy. In the circulation, due to the involvement of multi-party, making the data transfer control is poor, the risk of data leakage is intensifying.

The "Action Plan for the Promotion of Big Data Development" issued by the State Council in 2015 clearly pointed out that it was necessary to guide the cultivation of large data exchange market and encourage the market participants in all aspects of the industrial chain to carry out data exchange and transactions and promote the flow of data resources. The regional chain technology in the development of data has a strong advantage, through the regional chain data positioning can determine the data ownership issues, and because of the development and application of encryption technology to ensure that the flow of data to find the two sides of the mutual privacy.

2.2 Social Governance

In the area chain, everyone can see the smart contract, because the code and status of these smart contracts are in the block chain (assuming the block chain is the main chain and open). From a user perspective, a smart contract is usually considered an automatic guarantee account, for example, when a particular condition is met, the program releases and transfers funds. In short, a smart contract is similar to a web server, but unlike a web server, a smart contract does not depend on a particular hardware device. In fact, the code for the smart contract is executed by all the mining equipment. It is precisely because of this feature that is sufficiently transparent, regional chain applications can be used for scenarios such as securities registration and clearing, banking and other high creditworthiness.

2.3 Decision-tree Application

DTC based on the stored enterprise data, through the side-chain multi-level algorithm processing, can form a decision-making decision-making tree decision-making tree. On the basis of the decision tree, it can be developed with enterprise-centric enterprise applications, that is, relying on the main chain of DTC, through the side chain based on the enterprise scene as the core of the application, these applications can be through the main chain of information Interaction, so as to obtain the relevant algorithm of the main chain, from top to bottom, forming a strong expansion of the "neural network system."

Chapter Five CONCLUSION

Data chain is a block-chain technology integrated application platform, with tree-like layered, three-dimensional multi-chain architecture, while adding regional chain technology 2.0 as the core of the intelligent contract platform, distributed application of the underlying protocol and other innovative technologies The DTC's goal is not only in the application of data processing for the regional chain, in our development strategy, DTC will become the regional chain of circulation media, that is, the regional chain "bit currency." To this end, DTC R & D and community hope that with the like-minded friends together for the development of DTC continue to forge ahead.