Fractal Core：A Decentralized System For Token Economy

Fractal team*

v 0.1

Abstract: This paper proposes a public chain system that supports the development of token economy as the primary goal. The system uses the DPOS consensus mechanism to ensure the balance between decentralization and efficiency of the system. Map-Sidechain is the core mechanism of this system. Users can easily map various types of assets to the Fractal main chain, or create various types, heterogeneous or even single-node sidechains according to their own needs. Users can create sidechains themselves or purchase sidechain service from providers to reduce development and maintenance costs. Token economy needs to support the innovation of the business model in the blockchain industry and the migration of the existing business model to the blockchain world at a lower cost, which is the original intention of the Fractal system.

1 Introduction

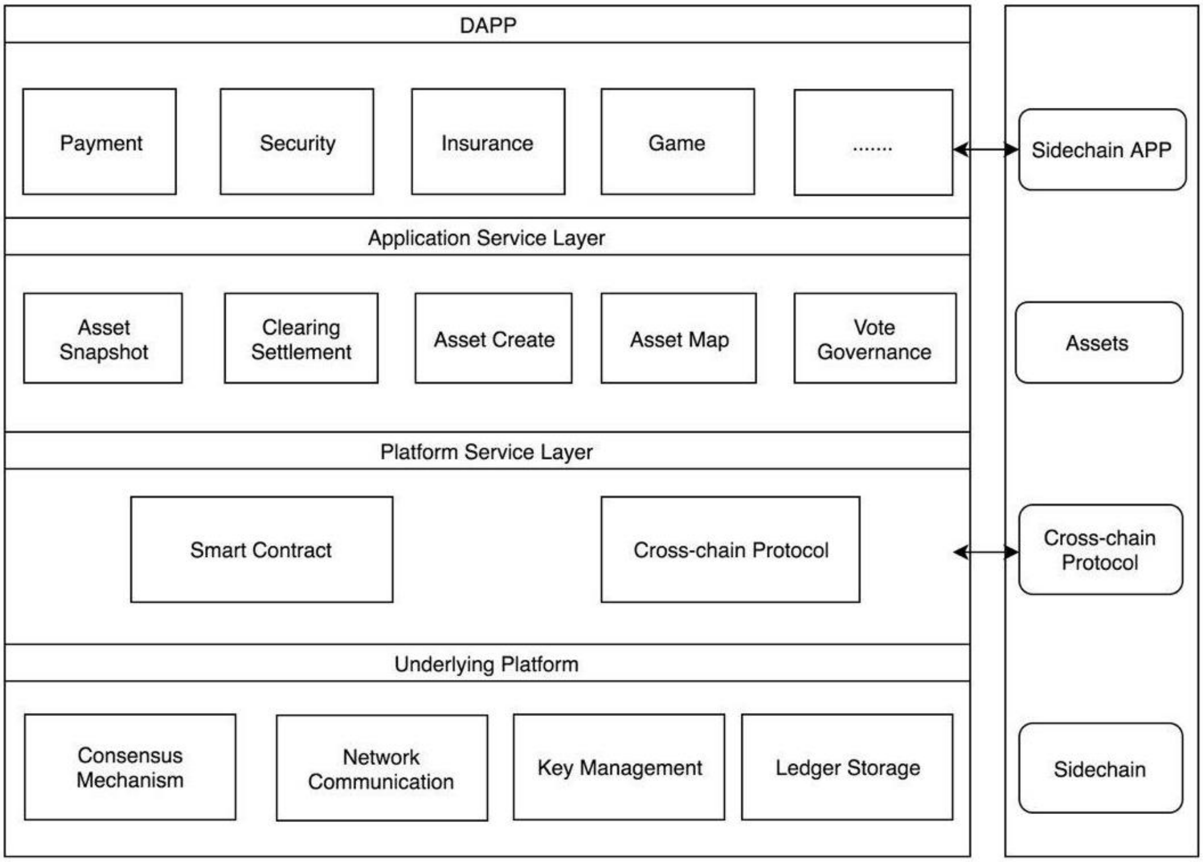
Advances in the level of technology have led to constant changes in human economic activities and social forms. Along with the explosive development of Internet technology, the demand for more convenient, secure and decentralized value exchange means has spawned the cryptocurrency[1, 2] boom represented by Bitcoin[3].

The cryptocurrency industry has evolved rapidly since the popularity of Bitcoin. First, there have been different types of cryptocurrency (Coin). With the birth of Ethereum[4] and the rise of ICO[5] later, the Token began to be issued and traded on a large scale. As a “certificate of circulated encrypted digital stake”, Token is the key to improving the efficiency of the traditional business model in the blockchain[6, 7, 8]. However, most of the practice of token economy[9] has halted at the ICO level. ICO is essentially a financing act which is not enough for token economy. ST (Security Token)[10] is trying to solve many of the inherent weakness of ICO to make the digital assets into mainstream. ST has many significant advantages, such as simplifying the authentication of qualified investors and compiling regulatory rules from different countries into smart contracts[11, 12] to realize the automerization of KYC and AML mechanisms. The future development of the token economy quite promising with the continuous innovation.

*Email: team@fractalproject.com

The goal of Ethereum is to become a platform for decentralized application. However, Ethereum cannot host the future growth of the token economy neither for design purpose nor actual performance. Despite the rapid development of the blockchain industry, there has not been an influential underlying platform that supports the development of token economy as its primary goal.

Fractal is a public chain project jointly initiated by FCoin digital asset trading platform and a few token economy supporters, which will support not only FCoin's own practice and exploration for token economy, but also the core aims of the future development of token economy. Fractal Core is the first core product of the Fractal project with the basic functions required for a high-performance public chain, including efficient consensus mechanisms and smart contracts, while endogenous supports for Token's issuance, circulation, dividends, and voting, various kind of community governance functions. In addition, through a flexible Map-Sidechain mechanism, Fractal system can map any type of real-world assets to Fractal and achieve efficient circulation and diversified governance through sidechain mechanisms.



Fractal Core Overall Architecture

2 FToken(FT)

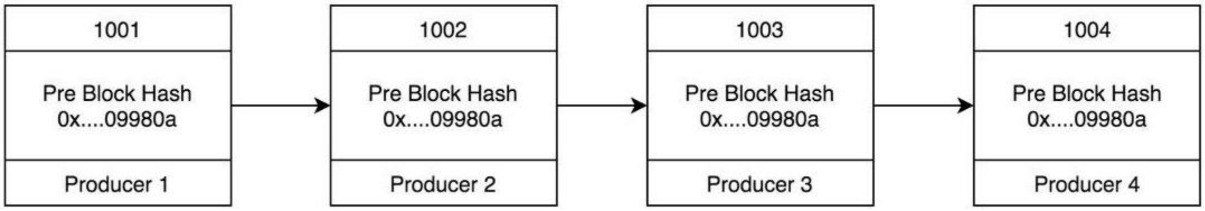
FToken (FT) originated from FCoin Token which is both the equity representative of FCoin digital asset trading platform and Fractal Public Chain. It completed the release of the 5 billion FT[1]through "Trans-Fee Mining" and "Pre-release Unlocking" mechanisms. Now the release of FT has terminated, there will be no new FToken even with the upgrades of FT brand.

3 Consensus Mechanism

DPOS is a consensus design borrowed from the representative system allows it to achieve both decentralization and efficiency, which has been widely used and proved in the practice of blockchain.

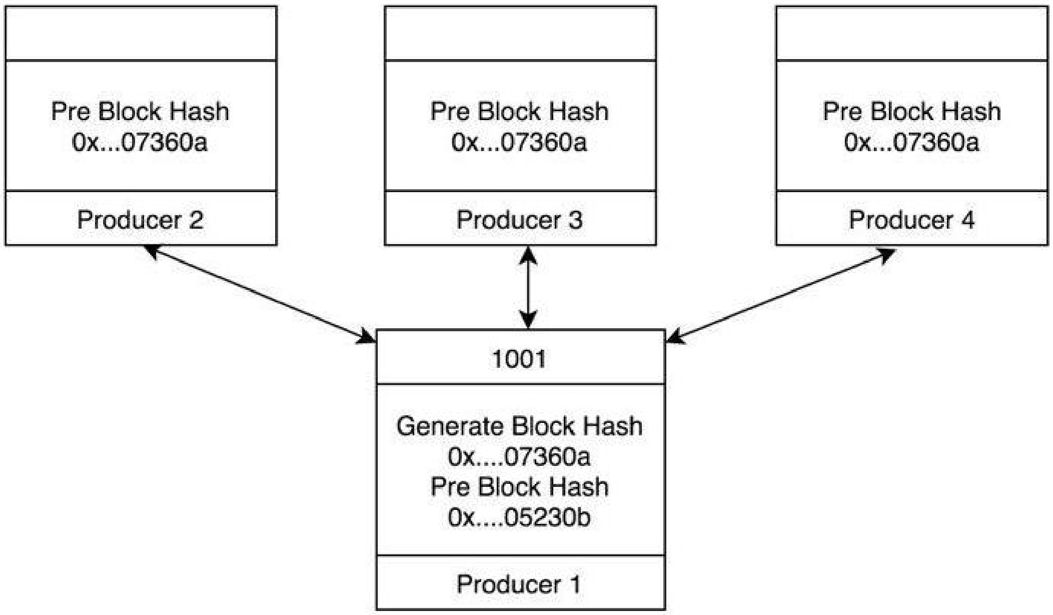
Bitshares' DPOS consensus mechanism[13] initially consists of 101-witness nodes which are trusted nodes elected by the community. Any user holding a token can participate in the process of voting and electing witness node. In the end, the 101-witness node with the most votes will be responsible for the production block. The fundamental purpose of the election is to select the users who are most beneficial to the development and operation of the project through the voting of each node. In the early stage of the project, the excess of the witness nodes may lead to the insufficient voting appeal to complete the election. Hence, we will gradually elect more witness nodes along with the increase of system user. Witness nodes are voted by FT holders on a regular basis. The more FTs you hold, the greater right to vote.

Traditional DPOS (based on graphene technology)[14] uses a random witness node block-generation order under generation speed of 3 seconds, if there are 6 witness nodes, more than 2/3 of the witness nodes need to confirm the transaction, with a total transaction confirmation time of 12 seconds.



In order to speed up confirmation time, we drew on the BFT[15] improvement of EOS, to allow the immediate confirmation once new blocks received. The block will be considered undeniable once 2/3 of witness nodes confirmed, which shortens the confirmation time to 3 seconds.

[1] For details please refer to: ftoken.com

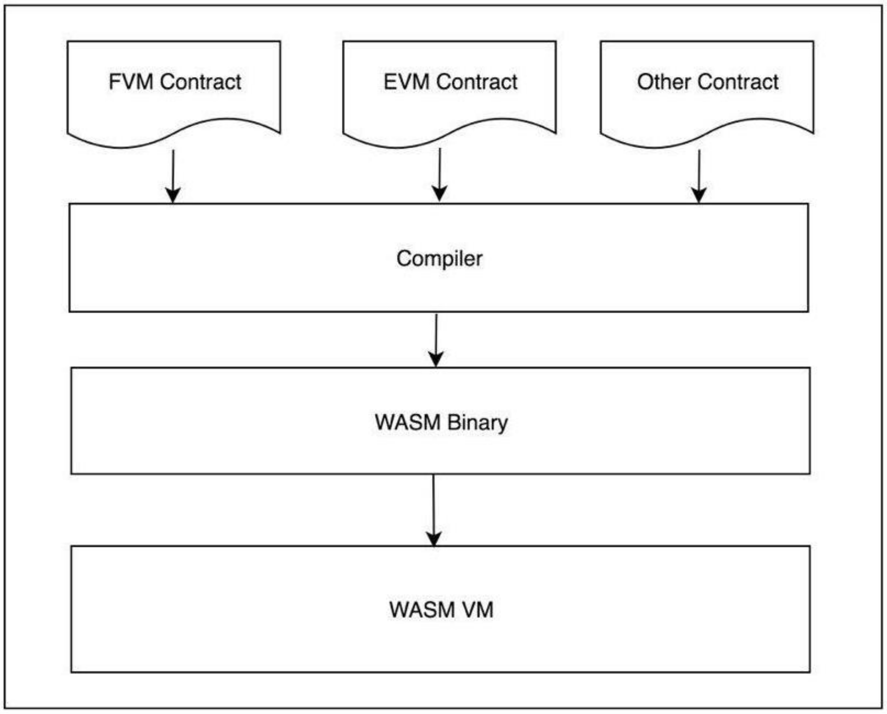


4 Smart Contract

Fractal Smart Contract Virtual Machine (FVM) is based on WebAssembly (a binary instruction format based on stack virtual machine, WASM for short), which can be used in various languages such as C/C++, Go, Rust, Java, JavaScript, etc. for the convenience of smart contract applications developing.

The near-native execution speed, the mature development community and toolbox make WASM be one of the best underlying technology choices for smart contract engines. Ethereum's next-generation virtual contract engine EWASM, is also moving in this direction. Hence, EVM can also access Fractal easily.

The underlying of Fractal smart contract provides a large number of APIs for developers and users including features like encryption algorithms, systems, blocks, databases, account assets, transactions and messages, which has laid a solid foundation for DAPP in various application scenarios.



5 Map-Sidechain Mechanism

There are two cores of the Map-Sidechain mechanism, one is Map and the other is Sidechain. The Map-Sidechain mechanism works as follows:

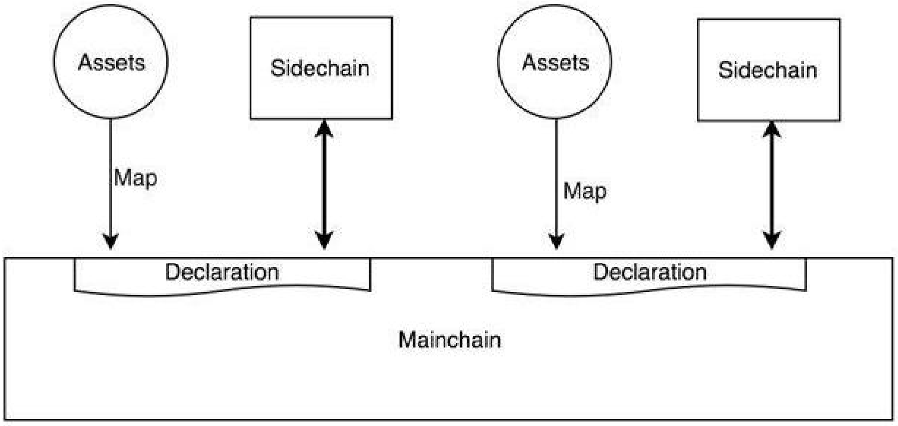
The first step is Map: create a special contract of type “Declaration” on the Fracal Core main chain and complete the initial release of the new token in the declaration. The Map Creator can attach a description or proof of the mapped asset to enhance the validity of the declaration.

The second step is Sidechain[2]: Create a sidechain contract under the Map declaration. The deployment and operation of the sidechain must be compliant with Fractal technical specification, and completed by the Map creator himself, or purchased the related services from the sidechain service provider.

The major role of Map mechanism is to allow assets outside the Fractal system to establish ownership and realize its free circulation in Fractal. It is worth noting that the Map creator itself will guarantee the authenticity and effectiveness of the assets. Map mechanism only serves as a public registration but will not care or guarantee the authenticity and validity of the assets. The major role of Sidechain is: First, to obtain massive parallelism ability to improve system load, so that Fractal ecology will not be subject to the performance of the main chain. Second, to realize a customized,

[2] Please refer to Fractal Core technology white paper for technology specification of Sidechain

or free transaction fee in order to significantly reduce user participation threshold. Third, to realize the customized functions and internal governance needs based on asset Map creator's requirements.



The Map mechanism is the core mechanism for realizing token economy while Sidechain is the key for realizing Fractal's ecological diversity to meet the diverse needs of token economy.

Take the mapping of btc to Fractal on a Bitcoin address as an example:

(1) Mapping assets: Create a declaration in the Fractal main chain and sign it with corresponding FT private key, include the proof of ownership as part of the declaration at the same time, such as using the private key corresponding to btc address to sign the content of declaration.

(2) Create a Sidechain: Create Sidechain contract under this declaration, the deployment and transaction processing of the Sidechain will be completed by the creator (the creator can also purchase services from the Sidechain service provider).

(3) The Sidechain can implement a special redemption transaction, allowing any address in the Sidechain to be redeemed by signature. After the redemption transaction is issued, the asset map creator will complete the transfer of the native asset from Bitcoin main chain, which means the completion of btc transfer.

Take the ownership mapping of a website as an example:

Sign the declaration with the private key of FT Main chain and include the ownership proof as part of the declaration, such as placing the signed declaration at the end of each page of the website and attaching a link.

The above examples are only intended to illustrate the feasibility of the declaration, not to define a specific style of the declaration, or guarantee the proof of all declarations. Different declarations are required according to the types and characteristics of the assets. A third-party organization needs to be introduced to enhance the proof of the declaration when necessary.

6 Transaction fees

Transaction fees have become an unavoidable topic in the current public chain ecology. The transaction fees of the Bitcoin network continue to rise, which is far from being “close to free”. And once the volume on Eethereum network increases, the transaction fee cost will rise rapidly, which will bring great obstacles for Token traders and application developers to create a diversified business model. Free trading is what we need most, but for the decentralized public chain, the reality is even without considering the interests of the trade packager, free trading will be vulnerable to malicious attackers for attack costs.

The transaction fees module of Fractal main chain is similar to the classic blockchain, which means the basic forwarding and packing fees will be agreed according to the transaction size. In addition, when the transaction increases and exceeds the capacity of one block, the block packager can choose to preferentially package the transaction with higher “value” according to the transaction fees.

The main chain transaction fee is only part of the Fractal network. The highlight of Fractal is its Map-Sidechain mechanism, which will create a large number of heterogeneous, even single-node sidechains. These sidechains can regulate its own transaction fee plan and blockchain architecture based on the nature of the service provided. In order to support certain business scenarios, the trading-free mechanism will emerge on a large scale in the Sidechain ecosystem. Usually, the Sidechain operators can profit from other upper layer applications rather than transaction fees, which can be used for the cost of server pressure and defending against malicious attacks.

7 Incentive Mechanism

Since the release of FT has terminated, there will be no new Token rewards for Fractal Main chain. The revenue of the witness node are mainly from:

(1) The Witness node will receive 20% of the transaction fee from its packaged transactions, while the other 80% will be regularly allocated to the FT holder.

(2) The Fractal system encourages the witness node to become a sidechain service provider. Stable witness node performance is a powerful endorsement to impress the customers.

8 Token Equity

Token is a circulatable proof of encrypted digital stake, consisting of three elements: equity, encryption, and circulation. Dividends and voting functions are the embodiment of Token’s equity.

In Fractal, FT is the token both represents the equity of the FCoin platform and Fractal ecology. It not only can obtain transaction fee revenue from FCoin exchange, but also participate in witness node campaigns, community governance activities, etc. in Fractal, along with the 80% transaction fee revenue from Fractal main chain. The Fractal public chain endogenous supports the issuance of the on-chain asset. Tokens representing on-chain assets can be traded, transferred, paid, voted, and destroyed. They can be circulated both in the main chain and across chains, and also can be transferred, created, and destroyed through cross-chain protocols.

The asset issuer of Fractal public chain can easily distribute dividends and develop a variety of strategies to expand ecology based on Dividend Module, as well as the development of insurance, lending, crowdfunding, etc., or financial derivatives. Voting is also a core function of the token equity. Asset issuers can formulate and implement relevant rules through smart contracts, so that Token holders can easily participate in community governance based on voting modules.

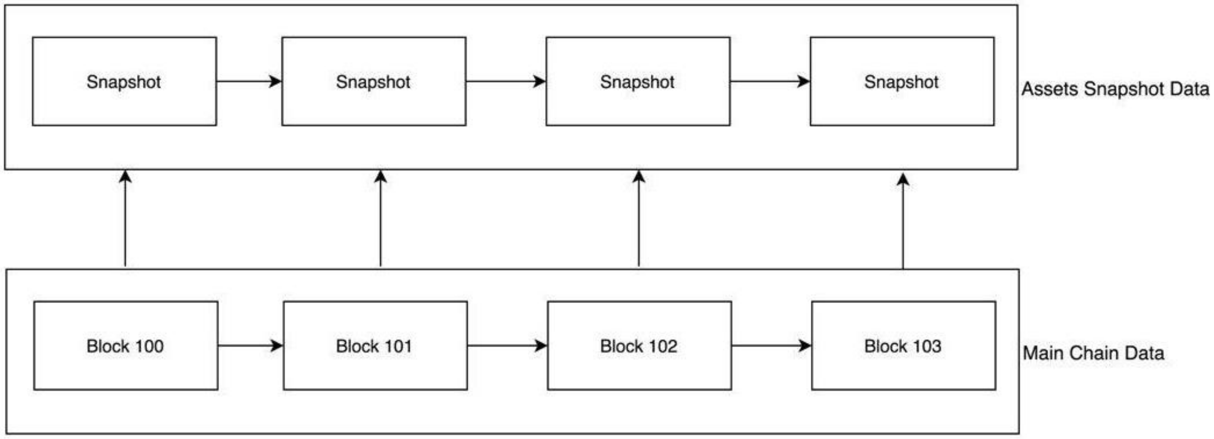
The FCoin trading platform will become a typical scenario of Fractal, the dividends mechanism (refer to the FCoin whitepaper), community-based autonomous features such as voting will be fully supported by Fractal.

9 Snapshots

The blockchain system itself is an elegant financial clearing and settlement system. However, due to the limitation of storage scale, most blockchain systems currently only store the most necessary clearing data but not the redundancy like the mirroring at a certain moment. However, the implementation of dividends, voting and other rights usually based on snapshot data at a certain time.

Fractal designed the asset snapshot feature under this demand. The generation of each block can be understood as a single clearing on the chain, and the time of the block is the timestamp for each clearing. So, we can record snapshot data of all the assets on the chain when each block generated. Snapshot data will only be stored at the witness node or the sidechain vendor node because of the high cost threshold for saving snapshot data, and the historical data can be deleted accordingly. The asset issuer can purchase from witness node or sidechain vendors for snapshots services when needed.

Asset snapshots can be mortgaged into votes during voting for community governance. Since the asset transaction is real-time, if the real-time data was used for voting, a loophole in asset-reuse voting will occur. Fractal's voting mechanism is based on snapshot data at a certain time, and the snapshot API can also be used. The asset used by snapshotting will be locked by the voting contract until the end of the voting.



10 Sidechain Service Providers

For commercially understanding, if we see Fractal as a "basic telecommunications network", the Sidechain service providers are similar to "cloud computing" providers. Sidechain providers are a vital player for the Fractal ecosystem.

The development of the token economy requires a variety of blockchain implementations to meet the needs of different commercial organizations. Such a diverse ecology cannot be designed in advance, nor can it be supported by a single public chain. That's why we introduced Sidechain service providers which are driven by commercial interests to provide diversified sidechain products according to market demand, in order to meet the needs of different scenarios and customers.

From a technical point of view, the asset Map creators can implement, maintain and develop sidechains themselves, but the cost will be high in most cases. In fact, the functionality demand in many scenarios is similar, so the professional sidechain providers can provide more reliable sidechain services at lower cost.

11 Digital Asset Trading Platform

The digital asset trading platform is an important part for both the current blockchain ecology and the future token economy. However, the existing trading platform has been criticized for its non-transparency and centralized nature. Therefore, the decentralized trading platform has become a hotspot represented by BTS[3]. However, the natural demand for efficiency and order concentration makes it difficult for the development of the decentralized trading platform.

We believe this type decentralized implementation path is problematic, and the practice of decentralized trading platforms cannot be achieved overnight. The decentralized trading platform

[3] https://bitshares.org/

based on public chain projects for payment purposes are doomed to fail because the needs for payments and exchanges are very different.

Using Fractal's Map-Sidechain mechanism, we can easily find a path to promote the development of a transparent and decentralized trading platform. For example, we can map all kinds of digital assets to the Fractal sidechain and complete"blockchainization" of the internal clearing system of the trading platform by using the parallel and efficient consensus mechanism. In this way, we can provide a Fractal sidechain address for the asset of each user on this trading platform, to achieve a preliminary transparency. Furthermore, we can also try to develop the matchmaking system into a sidechain of Fractal. Through the continuous exploration and practice in the above directions, we can complete architecture transformation from a non-transparency, highly centralized digital asset trading platform to a completely transparent, centralized and decentralized combinate platform.

12 Conclusion

Fractal Core is an application layer oriented blockchain framework, which aims to promote the development of token economy as a set of effective underlying tools. First, we introduced an efficient DPOS consensus protocol for the Fractal system to ensure the balance between decentralization and efficiency. Then the most important part Map-Sidechain mechanism by which the owners of real-world assets can easily map assets to Fractal's main chain through a standardized declaration mechanism. After the completion of asset Mapping, you can create your own sidechain or purchase sidechain services, to build the underlying mechanisms and economic models on your needs. From a commercial perspective, the introduction of "sidechain service providers" can create a large number of business models that conform to modern business rules and the spirit of the Internet and promote the in-depth development of the token economy.

References

[1] Hileman G, Rauchs M. Global cryptocurrency benchmarking study[J]. Cambridge Centre for Alternative Finance, 2017.

[2] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction[M]. Princeton University Press, 2016.

[3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[4] Buterin V. A next-generation smart contract and decentralized application platform[J]. white paper, 2014.

[5] Conley J P. Blockchain and the economics of crypto-tokens and initial coin offerings[R]. Vanderbilt University Department of Economics, 2017.

[6] Swan M. Blockchain: Blueprint for a new economy[M]. " O'Reilly Media, Inc.", 2015.

[7] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. Work Pap. – 2016, 2016.

[8] Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world[M]. Penguin, 2016.

[9] Pazaitis A, De Filippi P, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed[J]. Technological Forecasting and Social Change, 2017, 125: 105-115.

[10] Blockchain for investors. What are Security Tokens?[EB/OL]. https://blockgeeks.com/guides/security-tokens/, August, 2018.

[11] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE symposium on security and privacy (SP). IEEE, 2016: 839-858.

[12] Luu L, Chu D H, Olickel H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 254-269.

[13] Larimer D. Delegated proof-of-stake (dpos)[J]. Bitshare whitepaper, 2014.

[14] Schuh F. Graphene Documentation[J]. 2017.

[15] EOS.IO technical whitepaper[EB/OL]. https://github.com/EOSIO/Documentation/blob/master/zh-CN/TechnicalWhitePaper.md, July, 3, 2017.