whitepaper

Abstract

DiQi (pronounced Dee-Chi) is a decentralized platform for smart property. It is based on a mutually verifiable distributed ledger (the “blockchain”) that enables bottom-up participation in financial markets and remittance networks. DiQi adopts a multi-role structure and permissioned blockchain that allows it to closely model real-world systems. It can therefore cater to business needs. Through the implementation of the DiQi system, traditional financial instruments can be integrated without introducing centralized intermediary risk. Powered by improved blockchain technology, which allows it to better support high frequency transaction rates and contract versatility. The DiQi system is capable of supporting sophisticated financial market and e-commerce applications within a decentralized structure.

Introduction

Until recently, financial transactions on the internet relied heavily on the existence of trusted third party verification (e.g. by banks and credit bureaus). In these trust-based models, validation and the provision of related transaction information are centralized, and both sides of the deal must place their trust in the third party.

In 2009, Bitcoin was developed as the first decentralized payment network and digital currency that did not rely on such a central authority. The Bitcoin network is based on a public ledger called the “blockchain,” which captures the transactions processed and enables users (the “Bitcoin miners”) to mutually

verify the validity of each transaction using a decentralized consensus algorithm. The innovations that Bitcoin introduced have drawn significant attention from markets and governments. Several other implementations of the idea of decentralized value transfer systems using the blockchain have sprung up accordingly (the “altcoins”), although Bitcoin remains the largest in terms of total market value.

Bitcoin, being the first experiment that solved the the centralization issue, has to compromise in several areas. One of these major issues is the speed of transaction.

Scalability issues and regulatory concerns have been the most serious growing pain for blockchain applications in the financial market. Some financial service entities require permissioned ledgers for their business needs because of their contractually binding responsibilities and legal accountability for the transactions that are processed through their system. Further weaknesses of Bitcoin in the e-commerce industry are related to transaction frequency and currency volatility. Bitcoin’s trading frequency is currently bounded at 7 transactions per second. Bitcoin’s price has also fluctuated in the exchanges because of market speculation and regulatory concerns.

One of the major concerns with Bitcoin is its economic incentive to monopolize mining power. If a single entity contributed the majority of mining power, it would be able to manipulate the blockchain and rewrite the history (“51% attack”).

In contrast, the DiQi system establishes the true usability of digital currency. By focusing on improving blockchain technologies, the DiQi system has provided practical solutions that will allow it to scale up as needed and closely match real business needs in the financial markets and e-commerce industry.

Extensions to Bitcoin

DiQi system utilizes the same blockchain technology underlying Bitcoin, but makes several important extensions.

Same as Bitcoin

- blockchain

- Proof-of-work
- similar transactions and block format

Extensions

- multi-token architectures
- multi-tier permission system
- alliance-based permission system
- improved mining difficulty

Features

- Multicurrency and tokenized assets
  - DiQi natively provides multcurrency capability. DiQi allows issuers to issue multiple types of currencies. Bitcoin is a single currency system.
  - DiQi's system is similar to a colored coin system. Multiple colors can coexist on the same network. Multiple type of tokens can coexist on the same network.
  - A colored coin may be used for many different purposes. Colored coin tokens may be used to represent financial instruments, physical assets, or digital assets.
    - examples:
    - financial instruments
      - shares
      - bonds
      - debt
    - physical assets
      - car
      - land
      - house
    - intangible assets
      - copyright
      - music
  - Each type of coin can only issued by the same issuer.
- Member-only transaction for coins of a particular color
  - an issuer can require that only the approved address can transact the coin issued by the particular issuer. This is called member-only transaction

    - an issuer can make an address a member by sending colored coin to that address. This is called activation of a member.
    - this feature is optional. An issuer can decide to disable this feature.
- Change in transaction structure
    - DiQi has a similar transaction structure as bitcoin. However, two fields are added. One is the color field. The other one is the type field.
    - Different types of transactions include:
        - normal
        - mint
        - vote
        - license
- Change in the block creation time
    - DiQi's target block creation time is 15 seconds.
    - Bitcoin has a 10 minute average block creation time.
    - Many applications benefits from a sub-minute block creation time. For many applications, users are unwilling to wait for 10 minutes for confirmation. Waiting for 15 seconds for confirmation is a big improvement.
    - DiQi's 15 second block creation time increase tps (transactions per second) substantially.
    - Currently, Bitcoin transaction volume is ~7tps.
    - Block is only created when there is a transaction. No block is created when there is no transaction. This helps reduce the blockchain size. This measure will substantially reduce the amount of data during the early days of a private ledger.
- Multi-tier multi-centered: There is an alliance with one or multiple members on a DiQi network. Alliance is responsible for mining and creating blocks. Alliance member has the power to license issuers. Issuers have the power to issue colored coins. Each alliance member can license one or more issuers. Users can use one or more currencies. The currencies are tradable on the platform.
- Multicurrency: DiQi is a multicurrency system. Bitcoin is a single currency system. Multiple currency can coexist on DiQi network. Minting cap for a single currency is 10 to the power of 10 (10^10). The issuer may optionally creates minting schedule for its currency.

- Smart Contract: DiQi provides smart contract capability that is optionally extensible for the customer need. Just like Bitcoin, a simple stack-based script is provided in DiQi transactions. Unlike Bitcoin, customers have the possibility of accepting more flexible scripts. Bitcoin also provides scripting capability within its network. However, it is difficult to make any modifications to Bitcoin protocol. Most Bitcoin miners will accept only standard transactions. DiQi allows more flexibility for its customers.
- Confirmation time: DiQi's confirmation target time is set to 15s. This will increase the transaction volume cap and decrease the latency of confirmation. Bitcoin's 10 minute confirmation target time has been a major source of user acceptance issues.

Special Functionality

There are several special functionalities. These special functionalities are represented using special type of transactions. There is a field called "transaction type" in the transaction.

- vote to add new alliance member (aka: sendvotetoaddress): at least half of the current alliance members have to agree to add a new member. An alliance member may starts a new round of voting. If at least half of the alliance members voted and agreed, the new member become an alliance member.
- create new issuer (aka: sendlicensetoaddress): an alliance member may grant "issuer" permission to an address. Doing so is called sending issuer license to an address.
- mint (aka: mint): an alliance member and an issuer may create new coin. Note that coin of color id 0 is reserved for protocol use. Coin of Color id 0 is used as a token for alliance member to do their voting or issue license.
- activate a member: DiQi system has an optional member-only-transaction requirement. An issuer can require that only members can be involved in the transaction. In those case, the issuer has to send a small amount of colored coin to that address to activate a

member. Unlike the other special function, this function uses a normal transaction instead of a transaction of special type.

Roles in DiQi network

There are many distinct roles in the DiQi network, i.e. alliances, issuers, full nodes, and DiQi wallets. Each role has a set of different functionalities and permissions on the blockchain. A functionalities comparison is shown in Table 1.

Alliances: securing the network

DiQi adopts a multi-alliance structure for verifying transactions in the network. Each alliance member may comprise a group of DiQi users who compete with other alliance members for the right to validate the ledger and earn a transaction fee, based on computing power. Alliance members may coordinate with each other through a voting system to accept a new alliance member, or to ban a misbehaved alliance member. This co-existence of competition and cooperation between alliance members helps to secure the entire DiQi network.

Vote (sendvotetoaddress): alliane member can add new alliance member by voting. More than half of the alliance member has to agree to accept a new alliance member. The new member will have all the same rights as any other alliance member.

Send license (sendlicensetoaddress): alliance member can issue license to an address. The owner of the address can issue mint new coins of a certain color.

Issuers: enabling multiple currencies

Issuers can mint tokens of a certain color.

Hayek's theory on the "denationalization of money" helps explain why digital currencies in the DiQi network have value. The primary argument is that by allowing the private issuance of currencies, open market interactions will favor the most competitive currency. Accordingly, DiQi supports transactions in multiple currencies, and each currency is minted by an issuer with the authorization of alliances.

In the DiQi network, the issuance of currencies must fulfill one of two criteria: (1) the currency has a proven purchasing power in a pre-existing

e-commerce marketplace provided by or directly related to the issuer or (2) the currency has a pre-specified mining schedule and distribution policy. In the former case, the issuance of currencies in the DiQi network is merely a migration process from a central database into the blockchain by the issuer. The value of a currency is based on the credibility of its issuer and the alliances that approve it. Through authorization by these alliances, an issuer can provide multiple currencies. The issuer is responsible for the minting schedule and distribution policy.

Mint: This is the function that creates new coin

Activation of member: The issuers can optionally specify that only approved members can own the token it issued. In order to approve a member, The Issuers have to send 1 satoshi colored coin to an address to activate that address. The address is considered a member of this color from now on.

Full Nodes:

A full node is a participant in the DiQi network that makes a full replicate of all the transactions and blocks. However, the nodes have no role in minting or mining. In other words, an issuer is a full node with a minting license and an alliance member is a full node with the right to validate transactions and blocks.

DiQi Ancillary Services

The DiQi operations support system (OSS) is a powerful and productive user interface used by alliances and issuers. It serves as a tool for monitoring, controlling, analyzing and managing the DiQi blockchain and related operations. DiQi Blockchain Explorer (DBE) is a blockchain explorer for reading blocks and transactions.

Table 1. Functionality comparison of different roles in the DiQi network

	Alliance	Issuer	Full Node
Mining	O	X	X
Mint	O	O	X
Blockchain	Full blockchain	Full blockchain	Full blockchain
Wallet	O	O	O
Activate member	O	O	X

OSS	O	O	X
DBE server	Optional	Optional	Optional

Applications / Use-cases

Token systems in an e-commerce marketplace

A token system created in the DiQi network is suitable for use by e-commerce merchants. The marketplace operator can issue its own currency and the related transactions using that currency can be processed without a bank.

Online stores and e-commerce marketplaces that provide product or service information to users usually have a membership-based structure, because the marketplace operator may have responsibilities to their members that are expressed in a terms-of-service agreement. The DiQi network is a permissioned blockchain, and it natively supports multiple currencies and member-only transactions at its protocol level. Therefore, the issuer of a currency in the DiQi network can identify its members in the blockchain. A non-member will not be able to receive the currency without the permission of the issuer.

Frequent flyer program

The member-only transaction feature can also be applied in a points-based customer loyalty program for online stores. By adopting the DiQi protocol, the issuer can confine the use of its loyalty points to its specified members, without the need for a centralized database. Along with the multi-signature feature, DiQi can be applied to scenarios that require multiple entities to jointly issue a new token.

The problem of security and trust among the business entities can be solved by the decentralized blockchain system. In the DiQi network, a new currency can be minted by multiple issuers acting together. Using multi-signatures, this process is verified by issuers co-signing their minting action.

Global airline companies could jointly issue mileage points for their frequent flyer programs using the multi-signature feature of the blockchain, without a establishing a centralized alliance structure.

The blockchain performs better than a centralized ledger database in terms of its resistance to data forgery, censorship, or reversal. Furthermore, the total

volume of currency in circulation is transparent to network users. The issuer can easily prove to its customers that the currency is not being excessively minted.

Smart property rights

Multiple publishers may collaborate to create a digital copyright data store. The digital copyright is a form of ownership that can be encoded in the DiQi blockchain. Publishers can issue tokens that bind their copyright data. The decentralized structure of blockchain makes it impossible for anyone to change the information once it has been encoded.

Private equity marketplace

The DiQi network offers possibilities such as:

time based trading.

stop trading after a certain period of time.

member-only offers to accredited investors or approved investors.

member-only offers to customers who satisfied the KYC (know-your-customer) rule already.

Conclusion

In the long run, we believe that decentralized ledger technology will become the industry standard for a robust trading infrastructure. Cryptocurrencies like Bitcoin and other Altcoins are inspiring innovation, and current technology may well be displaced by more advanced technology, as happened when MySpace was overtaken by Facebook's growing momentum. By integrating value-based currencies into the DiQi network and improving the blockchain to better suit the real needs of business, we believe that DiQi represents the next generation distributed smart property platform that will support a wide range of applications in financial markets and the e-commerce industry, whilst working within a decentralized structure.