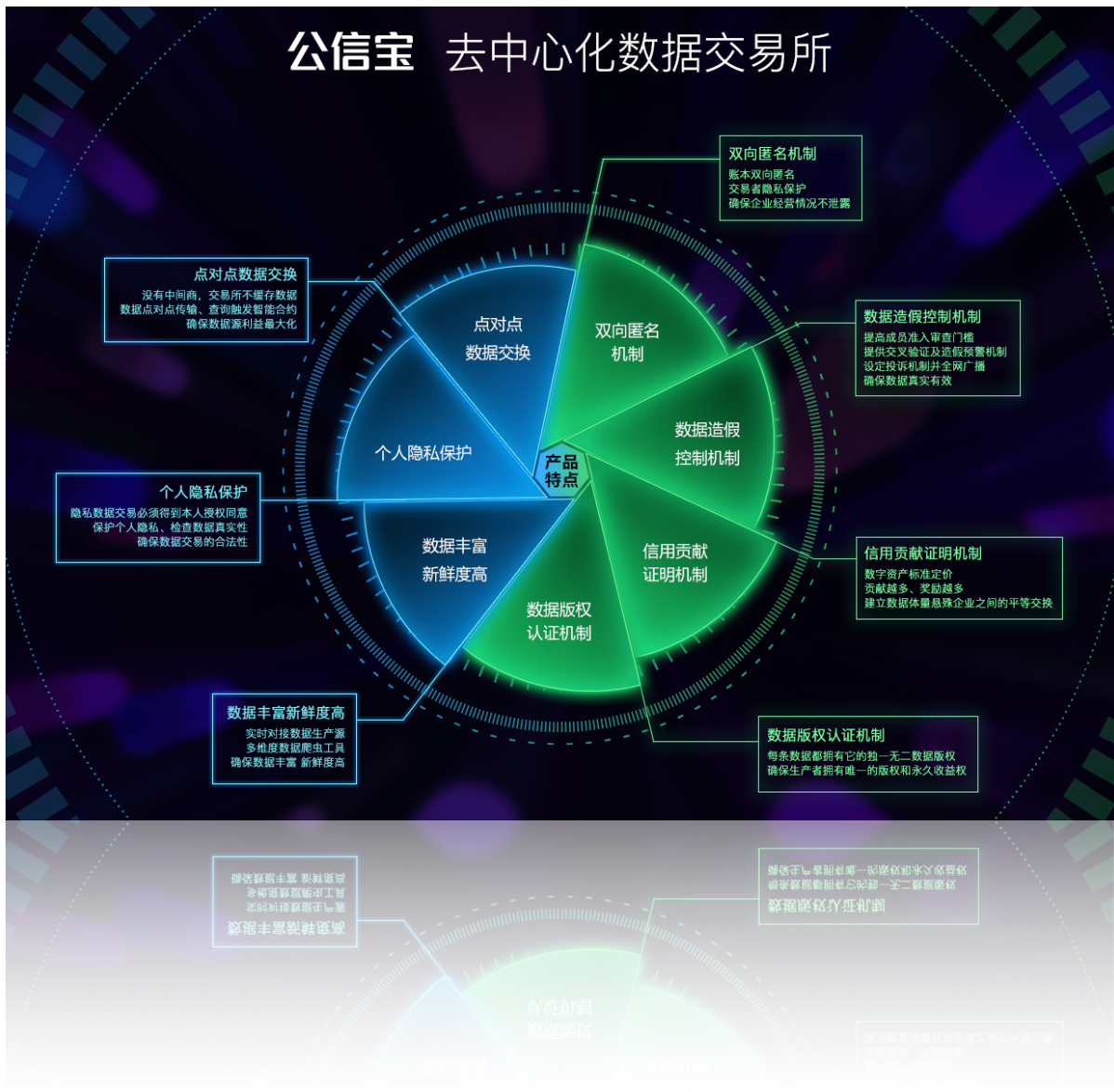# GXB Blockchain White Paper

Blockchain-Based Decentralized Data Exchange

China Hangzhou Credit Data Technology Co., Ltd. - 2017/2/2

1. Summary

An ideal data exchange shall enable both parties to a transaction store, transfer and exchange data with minimum risks and costs. We have redefined a new product named GXB, which is built upon the idea of decentralization and blockchain technology, to bring about the ideal data exchange. In the first place, GXB Data Exchange breaks the deadlock to get rid of "data precipitation" existing in traditional data exchanges. By virtue of decentralized peer-to-peer data exchange and asymmetric encryption of transactional data, no third party other than the buyer is able to access the data. Therefore, GXB Data Exchange can guarantee the best interests for the data source and safeguard the transaction privacy of both parties, who are kept anonymous by GXB. In addition, it enables the equal exchange between enterprises with a wide gap in their data volumes, facilitates authentication of digital assets ownership and effectively curbs data fabrication in data exchange.

GXB Data Exchange, a universal data exchange platform and an alliance chain based on the blockchain technology, is applicable to data exchange in all walks of life. Its typical customers range from pan financial enterprises (e.g. banks, P2P lending, automobile finance, consumer finance, petty-loan companies, etc) to government organizations and insurance agencies with data exchange demands. In order to better demonstrate its applications and more promptly access to the market, we first opt to use basic source data on individual credit as the primary digital assets and set customers in the pan financial field as the target group at the initial stage.

2. Glossary

GXB Coin: refers to the token used for settling data transactions at GXB Data Exchange. Its price is permanently fixed and its exchange rate to CNY is set at 1:1. GXB's operator serves as the acceptor to provide the exchange service between GXB Coins and CNY.

Node: refers to the client at GXB Data Exchange. Each client is an independent node and all clients are connected with each other via P2P network links.

Digital Assets: refers to the data traded at GXB Data Exchange, including but not limit to track record on loan repayment, overdue payment, lending, high-risk fraud, everyday credit, court enforcement, industrial and commercial credit, social security and housing fund contribution, consumption, bill payment to telecom operators, etc.

Trading Parties: refers to data buyers and sellers at the Data Exchange.

Data Source: refers to the source of data assets for sale at the Data Exchange.

Merchant: refers to the members who are qualified to transact at the Data Exchange, mainly including banks, P2P lending, consumer finance, automobile finance, petty-loans, insurance companies, telecom operators, government agencies and data companies.

Data Source Merchant: refers to the data source vendors, being GXB Merchants at the same time, who are qualified to sell data.

Alliance: refers to the alliance made up by a group of Merchants trading and exchanging their own data. Data within an Alliance shall only be traded between its members.

Alliance Member: refers to each Merchant who has joined the Alliance. Data owned by Alliance Members fall into the same category. Alliance Members are both vendors and vendees.

White List: each Alliance controls the members qualified for trading via the Whitelist mechanism. All members in the Whitelist are Alliance Members qualified for trading. Merchants added into the Whitelist become Alliance Members automatically.

Blacklist: Blacklist members are prohibited from any trading activities.

Smart Contract: A Smart Contract is a set of promises defined in a digital form, which contains an agreement that sets forth both parties are obliged to fulfill such promises as provided in the agreement. At GXB Data Exchange, a Smart Contract is initiated by the vendee requesting for data, in which specifies the type, identity, price, maximum number of entries, ceiling price and other conditions of the data to be traded. Once a Smart Contract is initiated, it is broadcast to the data source nodes carrying the same type of data and will be responded if such data are found at the data source. Then, the transaction is concluded if the final contract is successfully matched.

Broadcasting: refers to message transferring between the nodes distributed on the network through the blockchain network. Items to be broadcast may be a Smart Contract or a text message.

Peer-to-peer Transmission: refers to the peer-to-peer (P2P) technology, also known as the peering network technology. It is a new kind of network technologies. GXB adopts the P2P technology for data transmission instead of any centralized server.

Asymmetric Encryption: The very same secret key is used for both encryption and decryption in the context of symmetric encryption algorithm, while two separate secret keys, i.e. the public key and private key, are used for encryption and decryption when asymmetric encryption algorithm is applied.

Clean Network Commission: The Clean Network Commission is a non-profit unit under GXB to manage data fabrication. The unit holds an account to collect GXB Coins turned in as penalties and issues rewards to the best performers in each quarter and the members who have made a remarkable contribution to a clean network. The list is announced on a regular basis.

3. Current Issues in Data Exchange and Business Pain Spots

3.1 Issue of Data Precipitation

At present, "data precipitation" is seen in most data trading platforms (also called data exchanges) available in market. Data precipitation means data trading platforms offer data service via the API interface and sell the data obtained from other data sources under agency agreement as they do not have their own data. Each datum is cached once it is sold, thus gradually generating a cached database of grand scale. Then in the future, data trading platforms read and sell the data out of their local cached database, without having to request for the same data from the data source.

In this way, data sources can only sell the same data to a platform and make profit for once. It not only damages the interests of data sources but also fails to establish data ownership or to track data sources. What is more serious is that many data trading platforms are vulnerable due to poor security awareness; their cached databases are frequently liable to become the target of hackers who would steal the data. This is one of the ways how data is leaked.

In the field of internet finance, for example, there are strong demands for trading and exchanging of data on performance of financial agreements. However, once a trading platform precipitates its exchanged data, there is no way such data could be accessed by others. Because with all those data precipitated on the platform, if it branches out to lending and financing business one day, other market players will come to realize they have unconsciously cultivated a strong rival. Moreover, as such data are always sensitive and personal in nature, there will be serious consequences if those data precipitated on data trading platforms are recklessly sold or leaked.

3.2 Lack of Awareness of Individual Privacy Protection

There is still no unified understanding on many major problems concerning legislation on credit investigation so far. In particular, it is highly controversial when it comes to legislation on individual credit investigation system, e.g. identification of the scope of individual privacy, qualification audit of the credit investigation companies, etc. Therefore, continuous monitoring should be required in addition to the support of relevant laws and regulations on the protection of individual privacy. However, currently before such legislation is in place, data containing individual privacy has been traded

arbitrarily in the data trading market, without consent of the individual himself. Besides, the popularity of the emerging internet finance in recent years has directly triggered surging transactions of individual data. There lies a big market behind the scene.

3.3 Issue of Insufficient Data Updatedness and Data Fabrication

Think about the performance of internet financial agreement. Data precipitation is quite usual on data trading platforms or in big data companies. So, most financial service companies are unwilling to connect to such data trading platforms and play as a data source. Moreover, as many data transactions pay little attention to user authorization, data sources tend not to offer real time data to data traders. What buyers obtained is the data generated a few months or even a year ago, which leads to the insufficiency in data updatedness. Or even worse, many data directly come from the black market. Under such a dubious background, it is hard to remain unsuspected of data authentication.

Please refer to the article published by the official Wechat account of a financial magazine "Chaos in Credit Investigation: A Company Evaluated at Billions by Stealing and Selling over Thousands of Millions Data on Black Market".

4. **Data Trading Opportunities of Internet Finance Industry**

The current data trading market in the field of financial agreements performance is still a scene of chaos, there are no good solutions. Firstly, the national public authority (the Credit Reference Center of the People's Bank of China) does not take unified efforts to collect and evaluation these data. Therefore, the P2P lending and consumer finance industry have no choice but to perform credit rating by relying on the "small data set" offered by the credit investigation service providers (credit investigation companies, big data companies and credit rating companies). Those data are not updated, and it is hard to ensure their authenticity. As revealed on the internet, most of the credit investigation companies buy individual credit data from the "brokers" of black market. Data released from the black market contains a lot of fake information (the proportion may even go up to 90%). In addition to the black market, credit investigation companies also sell data secured from other data sources under an agency agreement. The data sold are cached (data precipitation), a typical centralized data trading idea. Each datum obtained from the data sources can only be sold for once, future earnings will not be paid to the data source companies, which severely damages the benefits of data producers. It is imperative to introduce a perfect solution to the credit investigation industry, which could solve the data quality issues while at the same time safeguarding the benefits of the data producers.

Moreover, the issue of "credit data island" in the financial industry has not been solved yet. Every day on average, over 30,000 P2P lending, consumer finance and petty-loan companies in China generate tens of thousands data on performance of financial agreements such as records on lending, repayments, overdue payments, blacklist etc.. These massive data do not give full play to their proper role. If a sound and healthy data exchange platform is built by bringing together the enterprises of the entire industry, it will greatly improve joint credit granting, control of loan leverage and reduction of bad debt, and bring huge benefits to the whole industry and the entire society.

5. GXB Data Exchange (on Product)

GXB Data Exchange is a blockchain-based decentralized data exchange, it will be able:

1. Not to cache/precipitate data from the data source;
2. To focus on safeguarding individual privacy;
3. To guarantee the data updatedness and accuracy to the greatest extent.

5.1 Introduction to the Business Process

The diagram above illustrates the general business process of GXB Data Exchange. The following text gives more details not shown in the diagram:

All data transactions taking place at GXB Data Exchange are in real scenarios. Here is an example:
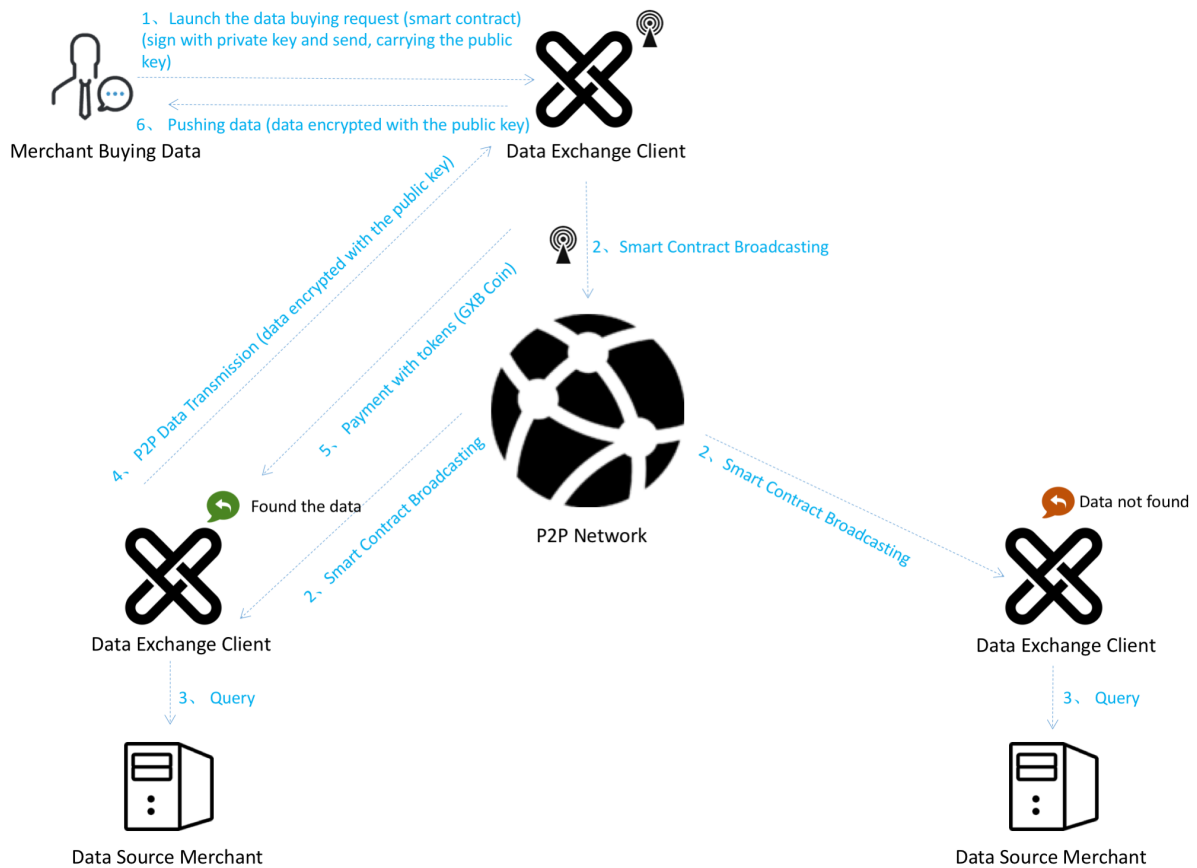
User A has filed an application for paying by installments to Merchant B (**Financial Service Company**) (**Merchant Buying Data shown in the diagram above**). When starting to process the application, due to the lack of User A's personal data, Merchant B initiates request at GXB Data Exchange for buying data on User A (**such request is a Smart**

Contract initiated by Merchant B's system via API interface of the GXB Client installed on its own server). Then, the data exchange client will determine whether the data requested contains sensitive personal data. If so, it triggers the individual privacy protection system and send a SMS to User A or a push message to User A's GXB APP (**if installed**) to request query authorization. If User A rejects, the process will come to an end and Merchant B fails to purchase the data. If User A accepts(**as is usually the case**), the data exchange will broadcast such Smart Contract to all Data Source Merchant client nodes accommodating such type of data, and each node will make an query in accordance with the terms of the Smart Contract. The node will be ignored if the required data on User A are not found; if the data are found, they will be transmitted directly to Merchant B's node as asymmetric encrypted data. Merchant B will automatically make payment to the data source with the token as specified in the Smart Contract. Now, Merchant B is finally able to retrieve the decrypted source data from its own node for further processing and utilization.

Note: **see 6.4** for the cryptology process in the business process above.

5.2   Free Market and Alliance Market

GXB Data Exchange market falls into two types:

5.2.1 Free Market

Free market is free in relative terms. After the fair price is set by the data source merchants and data are put on shelf for sale with the assistance of GXB, all merchants, except those on the blacklist, are allowed to call the interface to buy data.

5.2.2 Alliance Market

As compared with the free market, the alliance market is under the control of authorization. GXB sets up separate alliances for merchants owning data of the same type or from different vertical sectors, or even different alliances for merchants with data of the same type in a certain sector. Such efforts are made to meet the needs of different authorizations required by different alliances, e.g. the alliance of data on performance of financial agreements, Hangzhou alliance of data on performance of financial agreements, BAT alliance of data on performance of financial agreements, 5-certificate-in-1 data alliance, alliance of big data on health etc.

The prerequisite for becoming a member of any alliance market is its capacity to generate the specific type of data and the demand to purchase such type of data.

Such members will effectively trade or exchange data with other members within the alliance and finally realize healthy data sharing. Standard unit price for different types of data within the alliance is negotiated and agreed upon by GXB and alliance members.

5.3 Product Features

5.3.1 P2P Data Trading without Agent (No Cached/Precipitated Data)

As GXB adopts the blockchain-based decentralized trading technology, there is no third party in data transaction. What GXB provides is a P2P exchange scenario for all trading parties. For instance, a Smart Contract is broadcast to all merchant nodes (B\C\D...) over the whole network once Merchant A (the requester) initiates a data transaction request (i.e. the Smart Contract), the data will be directly sent to node A via P2P transmission if the required data are found on any of these nodes, and node A will automatically pay the token to the vendor. Asymmetric encryption channel is applied to the whole process, and the data purchased cannot be decrypted by any other third party except by Merchant A. Thus, data security is guaranteed. Moreover, what GXB Data Exchange offers is a transaction channel, and the blockchain only stores the transaction summary, certificate, digital copyright and other basic information required by the transactions, instead of the source data and encrypted source data used in the transactions. Therefore, it is impossible to crack the data by synchronizing all accounts.

5.3.2 Mutual Anonymous Authentication (anonymous trading account keeping)

As the blockchain account is open, transactions are traceable. But there are still demands for anonymous transaction in the field of data trading. Therefore, transactions on such blockchains need to stay anonymous. Take the internet financial enterprises as an example: they have strong demands for anonymous trading. Buyers do not what other merchants to know what they purchased, because they do not want them to figure out their credit investigation model. While sellers do not want others to know what they sell, because they need to protect their business privacy (e.g. loan balance, bed debt ratio, real interest rate etc.). At GXB Data Exchange, each alliance member involved in data trading is able to conduct two-way total anonymous account keeping on the blockchain (optional), i.e. the vendors do not know who purchased the data, while the vendees do not know who sold the data. Thus, privacy of both parties is fundamentally safeguarded.

5.3.3 The Proof of Credit Share Mechanism (for equal exchange of data between alliance members with wide gap in data volume)

It is hardly possible to exchange data between enterprises with wide gap in data volume before the introduction of a workable credit share solution. Because it is relatively unfair for enterprises with a large volume of data, and they do not care about the data volume of small companies. Hence, it is way too hard to establish data exchange between them. However, the combined data scale of 100 or even 1000 small companies cannot be ignored by large companies any more. Therefore, it is crucial to build a fair and impartial shared credit exchange system for enterprises with a wide gap in data volume.

The original Proof of Credit Share (PoCS) mechanism developed by GXB will thoroughly solve the problem. We set standard prices for each digital asset and data field (future fluctuation of asset prices shall be determined by vote by the administrative council and the overall market performance). A contribution value ("Share", similar to the computing power contribution in mining) will be calculated every time when a datum is queried and traded successfully. The larger data volume the alliance members own, the greater possibility there is for them to be involved in trading. So they are more likely to make greater contributions and obtain more rewards in the form of GXCoins. That is to say, more contribution, more data. While on the other hand, alliance members with small data volume often make relatively minor contributions, so, they have to buy sufficient GXCoins if they want to obtain the data they need. Consequently, under such a universally–accepted contribution-based background, all alliance members can happily do what they like in a fair and impartial shared credit exchange market.

5.3.4 Authentication of Digital Copyright (Authentication of Digital Asset Ownership)

As mentioned above, many data trading platforms and credit investigation companies would cache and precipitate a copy of data when they sell them. Then, they can resell the data to others as their own in the future, leaving the original data source with no choice but to sell each datum for only once. In this case, interests of data sources cannot be guarded, needless to say the authentication of ownership and traceability. The data traded at GXB Data Exchange will not be precipitated (cached), and trading revenue still goes to the original **producers** when the same data are put on for sale at the Exchange by those who purchased the data before. This all benefits from the Digital Proof of Ownership (DPO) developed by GXB Data Exchange.

DPO is the technical measures employed by GXB blockchain to control copyright authentication of the unique assets----data. Each datum will be allocated with a

permanent digital certificate to identify the data producer once a Smart Contract for data transaction becomes effective. Since then, the right to claim trading revenue generated by such data is permanently owned by the producer. Meanwhile, data ownership authentication and traceability come true.

5.3.5 Focusing on Individual Privacy Protection

Personal data trading at the data exchange must be authorized by the individual himself. The original intention of the alliance members to buy personal data is to get more information about the person for the purpose of managing lending leverage and risks pertaining to him/her. However, such transaction concerns personal privacy, and therefore requires authorization of the individual. The practice of GXB Data Exchange is to intercept buyer's request for data once a Smart Contract is initiated and determine whether the digital assets to be traded under the Smart Contract involves individual privacy. If so, the individual will receive a message on their phone or a pushed notification from their GXB app(authorization records shall be logged into the blockchain) and be asked to confirm the authorization. Once the authorization is granted, such Smart Contract is broadcast to the entire network to process queries and transactions.

In addition to eliminating the pain spot of the industry – difficulty in obtaining personal data in financial field, GXB will also be dedicated to the protection of individual privacy. We believe personal credit should be managed by the individual himself, and anyone or any organization must obtain personal authentication when they try to use such data.

Note: individual users may install (not compulsory) GXB APP to manage its personal credit. Registration on the app requires the name, identity card, phone number, bank card information, etc. After user's identity is verified, it will be logged onto GXB's blockchain and a dedicated private secret key will be generated. Then, all queries to his/her data are subject to his/her authorization via pushed notification sent by GXB APP or SMS on the phone.

5.4 No Challenge to State Regulation on Administration of Credit Investigation Industry

The utmost concern of the industry over the processing of credit investigation data lies in the possibility that its attribute to challenge the *Regulation on the Administration of Credit Investigation Industry* will give rise to substantial repulsion from the regulatory authorities and lead to legal issues. GXB Data Exchange does not precipitate or process

data, nor does it offer data assessment reports. Trading and exchanging of all sensitive data are subject to personal authorization and logged onto the blockchain, which means it will never violate the administrative regulations on individual credit. By virtue of P2P data trading enabled by blockchain, it puts an end to the chaos in current offline black market. The practice of reasonable and law-compliant data sharing between alliance members brings about a fair and impartial data trading and exchanging platform.

5.5 Control of Data Fraud

Currently, offline trading of individual credit data is rampant. Data generated by industrial and commercial authorities, banks and telecom operators, as well as information on identity, car, real estate and e-commerce transactions are especially popular. However, 90% of the data circulated in the black market are fabricated to make huge profits. This inevitably results in insufficient updatedness and dubious authenticity.

GXB Data Exchange curbs the issue of data fabrication existing in data exchange from the following aspects:

1)   Access threshold: as multidimensional data and data on performance of financial agreements cannot be accessed through web spiders, they need to be traded between all alliance members. GXB imposes rigorous restrictions on the qualification of alliance members, and only those with the capability to produce such data are eligible to join the correspondent alliance.

2)   Grievance proceedings: for data purchased at the data exchange, merchants may file complaints to the data exchange once they find seriously distorted or false data. The complaints, once verified, will be broadcast and synchronized to the whole network and saved permanently. Too many complaints filed against the same merchant will undermine its normal trading activities and reputation; worse still, the merchant will suffer severe punishment.

3)   Individual check: as discussed above, trading of data on individual privacy requires authentication of the individual. The Smart Contract is broadcast and synchronized to the entire network only after it is granted with individual authentication. Personal users may review the data successfully purchased under the Smart Contract on their GXB app or SMS. In the mean time, they are allowed to confirm the authenticity of the data, and voice their skepticism if there is any doubt.

4)   Penalty mechanism: when a certain number of complaints and questions are received and the probability of data fabrication is established by cross validation, such data will be converted into negative contribution value (-Share), which would offset the

contribution value (Share), i.e. the sufferer has to make more contribution to eradicate its -Shares. All its earnings will be transferred to the account held by the Clean Network Commission before it gets clean of all –Shares. Alliance members with high –Share value will be suspended and all its GXCoins be frozen.

Note: Earnings from the Clean Network Commission account are used to reward top performers in each quarter and members with the greatest contributions to a clean network. The list of award winners is announced on a regular basis.

5.6 Product Ecology Architecture Chart
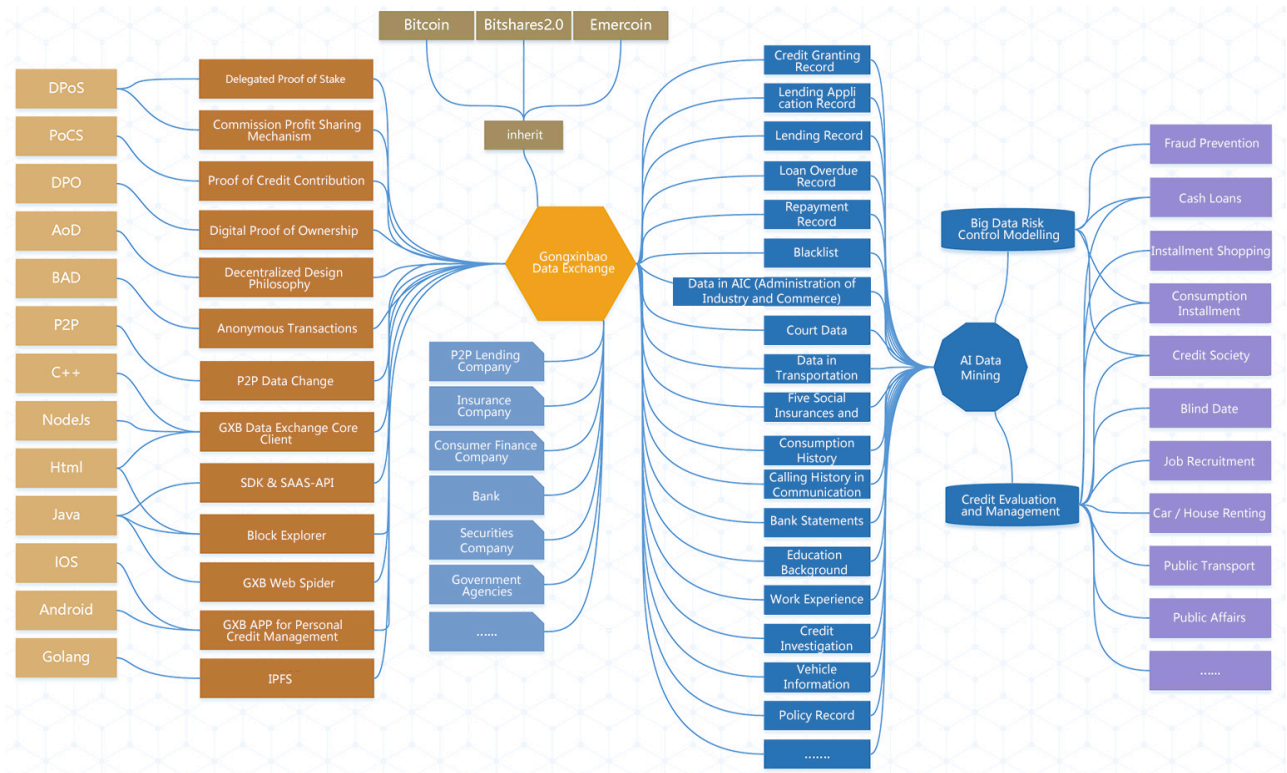
6. GXB Data Exchange (on Technology)

6.1 gxChain

The underlying blockchain employed by GXB Decentralized Data Exchange is gxChain, which is an independent blockchain developed iteratively by our team and an alliance chain (with access threshold) running on the public network (open internet). It is originally forked from Graphene (core of Bitshares2.0), based on which absorbs the functional agreement of Emercoin blockchain and anonymous treatment of Monero. More importantly, GXB team have made bold and resolute transformation according to our own business demands and thus developed GXB's exclusive code.

Here are the achievements made by our team:

1)   A new consensus mechanism (PoCS – Proof of Credit Share): used to solve the issue of inequality of alliance sharing between enterprises with a wide gap in their data volumes (see 5.5.3);

2)   A new digital assets ownership authentication feature (DPO – Digital Proof of Ownership): used to determine the ownership of each datum involved in data source transactions, so that each datum sold has an independent digital copyright certificate and is logged onto the blockchain (see 5.3.4);

3)   The asymmetric encryption feature for transmission of data transactions (see 6.4): to make data transactions safer and ensure there is no data leakage and precipitation during the whole process;

4)   Anonymous design newly developed on the basis of graphene to meet the demand for anonymous data transaction by both parties;

5)   JSON-RPC interfaces newly developed on the basis of light-wallet, so that each merchant can take all kinds of interactive activities as long as they have installed light-wallet. Merchants can install witness if they have the demand for data synchronization; it is much more convenient than ever;

6)   Private key signature for Smart Contract and asymmetric pairing feature for decryption of data received on the basis of light-wallet to ensure data security; data connection adapter and call-back mechanism to format and uniformly adapt to the input/output data type and reduce the efforts on transforming data source ------responses ; automated decryption of data with private key and push to the merchants through call-back when the data purchased by the merchants return to their nodes.

7)   In addition to the above, new features include data market, data type publishing, access audit, alliance management, penalty mechanism, sensitive data

management, individual privacy protection mechanism and many other functions on the blockchain tailored to business demands.

8)　　Some less significant features are not listed here.

Code References:

graphene: https://github.com/cryptonomex/graphene

graphene-ui: https://github.com/cryptonomex/graphene-ui

emercoin: https://github.com/Emercoin/emercoin

emcdpo: https://github.com/Emercoin/emcdpo

emcssl: https://github.com/Emercoin/emcssl

emclnx: https://github.com/Emercoin/emclnx

monero: https://github.com/monero-project/monero

6.2　Performance Optimization

Graphene absorbs the processing experience of LMAX Exchange. It facilitates up to 100,000 transactions per second, which benefits from the following key points of the core of graphene:

1)　　Put everything into the memory;

2)　　Put the core business logic into a single thread;

3)　　Put the operation of encryption algorithm (Hashing and signature) outside the core business logic;

4)　　Split the verification into state-independent and state-dependent check;

5)　　Use one kind of object-oriented data model;

In view of the demand for high frequency data transactions, optimizations have been made to gxChain – the underlying blockchain of GXB --- in these 5 aspects to support the frequency of millions transactions per second.

6.3　How to Solve the Issue of Blockchain Data Expansion

GXB solves the issue of data expansion with the following two methods:

Firstly, gxChain adopts separate witness and light-wallet mechanisms, same as in graphene. It may satisfy the demand to synchronize all accounts on certain nodes by running witness (full node), while most users only need to run light-wallet sized dozens of MB. Light-wallet can be linked to any witness. Further development is made on light-wallet by gxChain (see 6.1) and we have developed lots of JSON-RPCs, so that data trading between the Merchants, access to the data source and alliance market are all

realized through interface development on light-wallet, and no compulsory dependency on the witness is required any more. Certainly, merchants can install witness on their own servers and link right-wallet to such node if they wish to synchronize the full node.

Secondly, gxChain only stores entries like data transaction summary, certificate, digital copyright and other basic information required by transaction, instead of source data and encrypted source data for trading. Therefore, it not only reduces the block size, but also eliminates the risk of exposing account data when the encryption algorithm is cracked.

6.4 How to Prove There Is No Precipitation Data in GXB via the Cryptographic Method

In order to make clear this question, let's take the data transmission between the node of certain data vendee and the node of data source as an example:
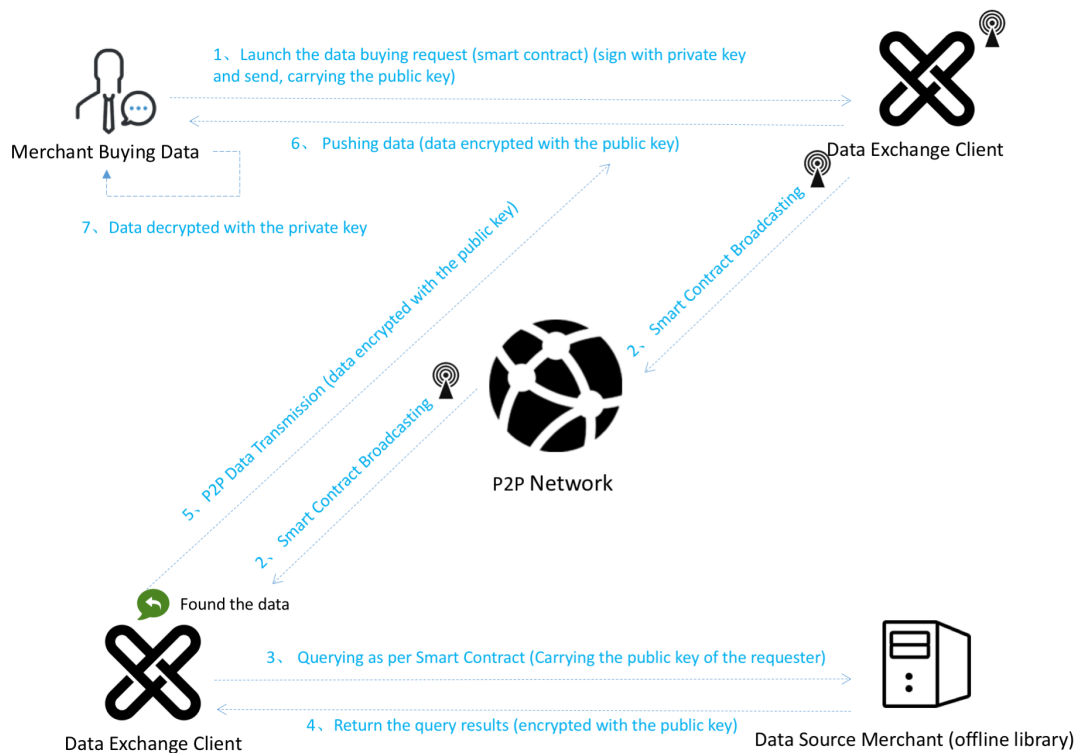
Merchant A, data buyer, signs the Smart Contract with its private key (which is generated on its own client and in its own way, not accessible by others), and sends the Contract with its public key. The Smart Contract is broadcast to all nodes on the network via the data exchange client. The nodes of the Data Source Merchants, as shown in the diagram above, receive the broadcast and make a query by calling the data interface of the data source. If the data source retrieves such data, it will encrypt the source data with Merchant A's public key and send the encrypted data directly to the node of Merchant A's client, where the data is pushed to its data reception interface. Then Merchant A is able to acquire the data by decrypting it with its private key.

Asymmetric encryption (SM2 elliptic curve algorithm) technology is applied to the whole process. Merchant A's public key is used in data encryption, and only its own private key is able to decrypt the data. The data cannot be decrypted even if data packages are captured by others during the process (or even captured by GXB, the data cannot be decrypted without the private key as well), which shall permanently safeguard transmission security during data exchange.