AdvancedCreditChain — Encrypted credit system white paper

Febuary 2017

"Our argument is not only circular, but something like it."

—Willard van Orman Quin

Content

Abstract

We present AdvancedCreditChain (ACDC), a generic crypto-credit system. At commercial level, ACDC focuses on less developed regions such as Southeast Asia and Africa, aiming to lay a solid foundation for SMEs. Technically, the biggest advantage of ACDC is that it can absorb any aspect of any kind of blockchain-based credit system that takes the various operations on the conventional blockchain as simple functional modules. Use these operations through the network shell to handle network layer tasks.

More importantly, ACDC supports metadata upgrades: the protocol can be evolved through self-correcting code. To do this, ACDC begins with a seed protocol to define a set of processes that will allow a retiring user to revise the code and fix the voting system itself necessary for the process. This is in agreement with Peter Schubert's Nomic game theory, which focuses on a set of introspective rules.

In addition, ACDC's seed protocol is placed on a pure Proof of Share (POS) system that supports Turing's well-established smart contracts. ACDC is implemented in the OCaml language, a powerful set of functional programming languages that provide high-speed, non-ambiguous semantics and syntax as well as the entire ecosystem. All of this makes ACDC a good candidate for formal proof of formality.

Familiarity with the Bitcoin protocol and basic cryptographic primitives are assumed in the rest of this paper.

1 Traditional business credit

1.1 Credit evaluation of traditional enterprises

With the growing scale of all kinds of business, the scale of the rapid development of enterprises in the industry, transparent, standardized credit system has gradually become an important factor to enhance business efficiency and effectiveness. Therefore, the subjective and objective factors that affect the ability of debt repayment must be taken as the research object to analyze the special factors of the formation of credit risk of different debtors Sex, to study its universality, which is the material basis for the formation of the principle of rating and source of ideas. The formation of credit risk factors are interrelated and interwoven, we must find out from the perspective of contact the formation of credit risk factors and the inherent logic of movement. The contradictory movement of credit risk factors must play a decisive role in the main factors and the main aspects of the main factors. Based on the universal connection of credit risk factors, the main risk factors and their position and function, Above reality, for reality. It is precisely using dialectical materialist methods of thinking that public can go deep into the very complex core of the credit risk system and find out the formation mechanism of credit risk.

Traditional credit evaluation of enterprises generally based on the following aspects:

（1）Enterprise's financial and financial status.

Financial status refers to a period of business activities embodied in the financial situation of fund-raising and the use of funds, it is a business - a period of economic activity during a comprehensive reflection of the results. The financial status of an enterprise is the assets and equity of a company on a certain date, and is the performance of a relatively stationary financial capital. The financial status is the status of the business activities reflected in the form of value, which is usually reflected through the balance sheet, income statement and related schedules. It is a financial reflection of the results of the business operations of the enterprise. In the American accounting profession, the balance sheet is often referred to as the Statement of Financial Position. Of the currently accepted balance sheet definitions, the balance sheet is also often considered a report that reflects the financial position of a company at a particular point in time. Obviously, the "financial status" here refers to the balance sheet status, which means that all the contents included in the balance sheet.
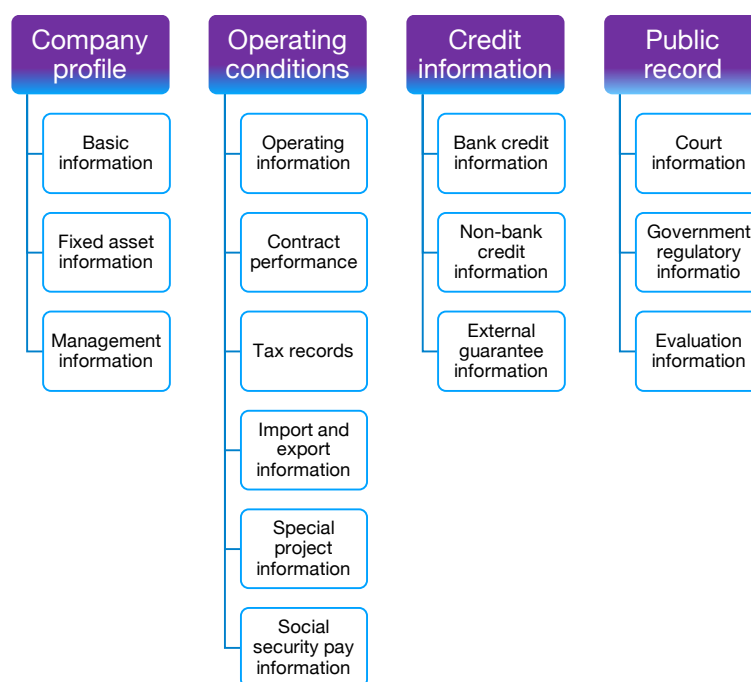
（2）Operating conditions.

Mainly includes the business information, contract performance, tax information and employee protection. Generally refers to the current labor law provides for the protection of labor and social security. Contract performance ability is the most direct business credit, cash flow information can also be seen, such as business conditions and many other aspects of the information. Current benefits refer to non-cash compensation used by enterprises in order to retain and motivate employees in the form of insurance, physical assets, stock options, training, paid leave, etc. The amounts listed in the system are calculated from the perspective of the cost of the company Considered, converted into the amount of display.

（3）Credit information.

Mainly corporate lending information. Corporate lending financing mainly refers to the financial intermediation between financial institutions and non-financial institutions, referred to as borrowing and financing, it is the longest history, the most widely used as a means of financing. Loan financing in many forms, according to different classification criteria are divided into many categories. An external guarantee refers to a commitment by my domestic institution to an overseas institution or a domestic financial institution with foreign investment to perform the repayment obligation on its behalf once the debtor can not pay the debts according to the contract.

(4)Public record.

The main emphasis here on the legal compliance of enterprises. Mainly on business and business owners contract review, legal incident handling records, compliance review to be more complicated. For compliance reviews, in addition to having to face static state laws, they are subject to the dynamic regulation of regulators. Any mistake, there is the risk of legal sanctions or regulatory penalties, resulting in significant financial losses and even loss of reputation. Legal compliance will involve environmental protection issues, safety issues, and even the new "Advertising Law" in September there will be compliance issues, such as what kind of people can be used as a corporate spokesman, an increasingly wide range of; Second, in the anti-commercial In the process of bribery, enterprises should deal with a series of judicial investigations. For the legal affairs without any jurisdiction, the investigation will be a big challenge. Furthermore, the financial affairs from multinational corporations to state-owned enterprises and private enterprises Enterprises have to meet the regulatory needs.

Company profile	Operating conditions	Credit information	Public record
Basic information	Operating information	Bank credit information	Court information
Fixed asset information	Contract performance	Non-bank credit information	Government regulatory informatio
Management information	Tax records	External guarantee information	Evaluation information
	Import and export information		
	Special project information		
	Social security pay information		

In the enterprise credit investigation phase of the investigation, there is often a certain degree of problem between the investigator and the enterprise. First of all, the above-mentioned legal compliance review of enterprises is very flexible. Strict compliance with corporate and reluctantly compliant enterprises, the actual implementation of the process there is a massive gap. In addition, many of the auditing information are not transparent, making the auditor's own credit has become very important; the credibility of the final audit material has also become a problem in the audit. Some companies have falsified, tampering records, etc. If these behaviors are not found, it will directly affect on the results of assessment.

1.2 The traditional credit industry's pain point

At present, there are two problems caused by the asymmetric information between investors and managers: the first is adverse selection and the second is moral hazard. One effective way to solve both problems is credit rating. Not only does the credit rating open up a channel for the information gap between the supply and demand sides, so that the capital market will not be able to function as a financial intermediary due to the asymmetric information, so that those in need will be able to obtain the necessary funds to engage in the business operations of each cow, Having funds providers' investments with the appropriate risk appetite also enhances the management efficiency of financial institutions and enhances the overall efficiency of the capital markets. However, whether

the credit rating is reasonable and the result of the rating is accurate depends largely on the scientific nature of the rating method.

The main obstacles to the current corporate rating are as follows:

(1) corporate credit rating has not been recognized by the whole society. At present, the economy of our country is in a period of transition. The concepts and old habits of the original planned economy still exist, and some are still deeply rooted. Some people still stay in the past with the funds allocated by the state finance, without paying any attention or even "relying on debts" The concept of "escape from debt" benefit from the stereotypes. Credit rating has started later, in the past two or three years in some provinces and cities began, is still in a "point" situation. At present, enterprises, including the government do not understand the credit rating, or have little or no prejudice, is still in a very difficult stage of promotion.

(2) lack of legal basis. The corporate credit poor farmers international industry management and business rules are basically blank, and the legal liability provisions are not perfect either. At present, only the "Decision of the CPC Central Committee on Several Important Issues concerning the Reform and Development of State-owned Enterprises", the "Regulations for the Administration of Enterprise Bonds" and the existing "Regulations on the Administration of Enterprise Credit Ratings" promulgated by the People's Bank of China in September 1999 are still in place. The People's Bank of China's corporate rating is still at the level of departmental rules. Lenders management, rating process and rating results have not yet put forward the norms. The business rules of credit rating, the corresponding legal liability of employees and so on have not yet been included in the scope of legislation, haircut lower level, the content is too thin, failing to reach the mandatory effect.

(3) The basic functions of credit rating and social "demand" there are differences, especially the beginning of the market to promote contradictions are particularly prominent. Credit rating is an effective means to reveal the market risk. Its basic function is to analyze the credit status of the economic organizations under evaluation, reveal the risks, make it public, provide public information to the society, and meet the needs of investors and regulators, It's rating results and quality, that is, the first goal of the operation is that investors and regulatory authorities use and trust rating results to provide them with decision-making reference. The current situation is subject to rating companies have high expectations of the level, a great "no AAA does not give up" trend. Second, there is an objective reason: the current national rating business has not fully rolled out the front door but has

become a "low-level", once the bidding market, there is no "high-level" Cannot short-listed, thus seriously affecting the normal operation and development of enterprises.

(4) The quality of the agencies themselves is less high, especially in the case of "less food, more predator" kind of situation, self-discipline can be even worse, and even escalating prices, there is a moral hazard."

There is a huge base of credit information in China, but the data are not shared. The information of credit reporting agencies and users is not symmetrical. Credit agencies and credit agencies, credit agencies and other agencies lack of effective sharing and cooperation, information silos serious problem, unable to achieve high-quality credit card industry data circulation and transactions, resulting in information asymmetry credit agencies and users. There is a serious problem of isolated islanding of information among interbank agencies. Massive credit data of credit institutions, consumer finance companies, e-commerce financial companies and other institutions in the financial industry have not yet exerted their due value, and the credit information outside the financial sector has been severed in the courts, government departments, telecommunications Operators and other agencies in the hands. The reason is mainly that the ownership of data in various countries has not been established yet and is under privacy protection concerns. All agencies would rather hold the data in their hands firmly and have no additional enthusiasm for data exchange and sharing. In addition to institutional reasons, the traditional credit reference industry also can not share data securely between agencies and industries because of the technical architecture. As a result, the issue of data silo in the traditional credit reporting work has not been solved yet.

Formal market-oriented data collection channels are limited, data sources battle cost a lot of costs. Credit data is different from other industry data. Users belong to the most important data tag related to the vital interests of enterprises and individuals. Therefore, credit data can not be shared and exchanged through traditional data exchange platforms. As a result, formal market-oriented collection of credit data channels is extremely limited. The traditional credit reporting agencies, through self-excavation, cooperation and purchase, proactively interface relevant departments and agencies to consolidate data from a limited number of scenarios to seize the high ground and opportunities in the development of the credit information industry. Therefore, competition on data sources is particularly fierce, which also directly causes the traditional credit agencies to spend a large amount of costs on data collection, resulting in a shrinking proportion of funds used for data analysis and credit product research and development, and credit agencies can not pay too much

attention to credit the quality of products, which in turn affect the level and credibility of credit agencies.

Data privacy protection issues prominent, traditional technology architecture difficult to meet the new requirements. The credit information industry in the era of big data has higher requirements for privacy protection and data security. The central bank issued a very personal cautious credit card, indicating that the regulatory agencies for the official release of personal credit there are still doubts, privacy protection, personal credit evaluation indicators are not uniform and other issues is still the most important central bank concerns. In addition, the gray industry chain of personal information transaction in "dark network" has become a pain point and a difficult point for investigation and handling by the regulatory department for its diversification, concealment and complexity. To this end, the People's Bank of China Credit Management Bureau explicitly instructed to strengthen the protection of privacy, require credit agencies to collect user information should be approved by the main body of information, and clearly inform the possible impact of such matters, the main body of information the right to request credit agencies will It incorporates the scope of refusals for marketing. However, the traditional credit information system technology architecture is of low concern to users, and does not guarantee users' data sovereignty from the bottom of the technology, thus it is difficult to meet the new requirements of data privacy protection.

1.3 Investment and credit situation in Southeast Asia and Africa

**Figure 1.4.** Sources of FDI finance in ASEAN, 2003–2015 (Millions of dollars)
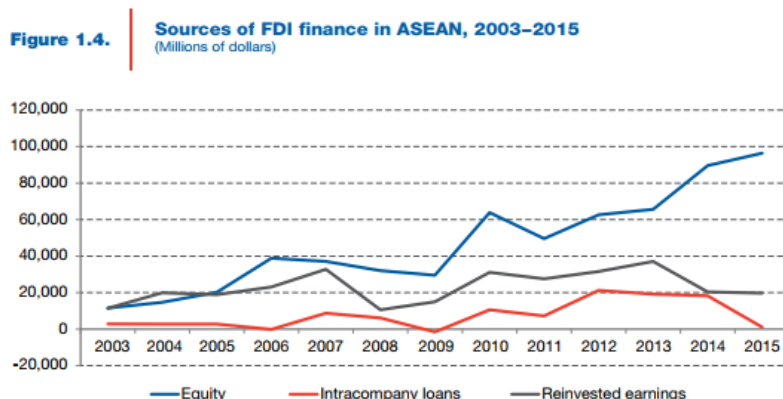
It can be seen that the Southeast Asian market is also increasingly capable of attracting foreign investment. Five countries will become the global investment destination of multinational corporations in 2016-2018. Indonesia, Malaysia and Vietnam rank higher in the list of the world's

premier investment destinations, with the Philippines and Myanmar made their first appearances. Foreign direct investment (FDI) inflows into Southeast Asia in 2015 were 126 billion U.S. dollars, up 1% over the previous year.
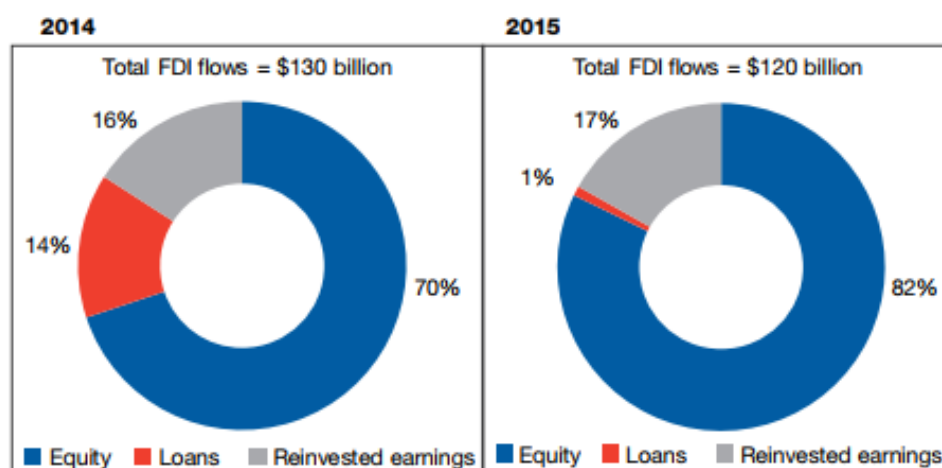
Direct investors were considerably more active in using equity capital to finance investment projects in ASEAN in 2015 as compared with previous years. In contrast, the intracompany loans component of FDI finance declined significantly, from 14 percent in 2014 to only 1 per cent in 2015, which contributed to the $10 billion decline in FDI flows (figure 2). The amount of outflows of intracompany loans (repayment of loans orprovision of new loans to affiliates and parent companies) was greater than the amount of inflows of intracompany loans to subsidiaries based in ASEAN, in particular Singapore and Thailand. Some outflows of intracompany loans supported the financing of investment in affiliates in other ASEAN Member States. In Singapore, the net outflows of intracompany loans went to destinations outside of ASEAN.

FDI projects, 2005 - 16 (percentage share)
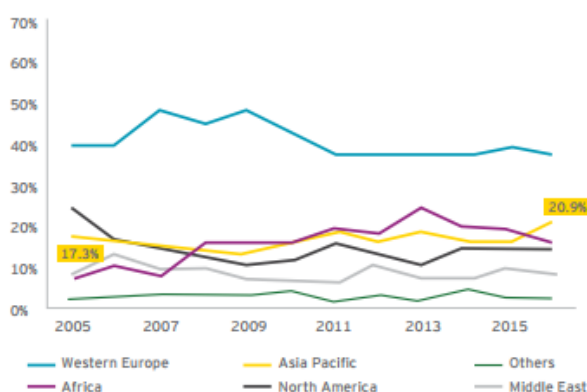
FDI capital, 2005 -16 (percentage share)

Legend: Western Europe, Africa, Asia Pacific, North America, Others, Middle East
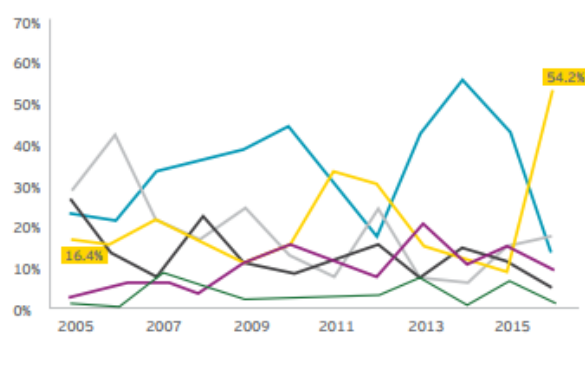
In a sign of diversification of Africa's investors, investmentfrom the Asia-Pacific region into Africa hit an all-time highin 2016, accounting for more than a fifth of projects andmore than half of capital investment. Companies from the Asia-Pacific region were also the largest contributors to FDI jobs to Africa. In recent years, China and Japan have beencompeting with other Western countries — including the US, to build influence on the continent. China-sourced FDI into Africa increased dramatically in 2016. With a 106% jump in projects, China became the third largest investor in the continent. In fact, this was the highest level of FDI from China across all three metrics, (namely projects, capital investment and jobs) since our Africa Attractiveness Program began. Almost a quarter of Chinese FDI projects were directed toward Egypt. In January 2016, the Chinese President Xi Jinping, visited Egypt during which his country committed to a US$700m loan to the National Bank of Egypt. China is also planning US$15b of investments across 15 electricity, infrastructure and transport projects in Egypt. Across Africa, Chinese investors took an active role in the TMT, automotive and business services sectors in 2016.

1.4 analysis of blockchain-based credit feasibility and necessity

Traditional data centers usually store data on a single central node. The central node is completely controlled by the data center, the data center can be free to modify, delete these data. The data center for the sake of profit, it is entirely possible to sell fake data, tamper with or delete data current data. Alliance mode is generally a number of small data centers attached to a large data center, small data centers and large data centers for data interchange. This model of small data

centers cannot trust each other, all the data through large data center exchange. The net result is that large data centers will place the blockchain as a decentralized distributed data storage technology. It's core value is to create a safe and trustworthy system that allows organizations or individuals who do not trust each other. Therefore, the introduction of blockchain technology, will be a good solution to some of the pain points in the above problems. First, at the enterprise level, blockchains can help us establish our own data sovereignty and generate our own credit assets. This is the basis of personal credit production, but also our future source of important assets and security, but also conducive to credit agency credit production costs to reduce. Now, with the exception of credit reference centers, ownership of user data is almost entirely mismatched, and they are held in the hands of major Internet companies, making it hard to control their own private data, let alone authorized. Moreover, each of these large Internet companies monopolized a market to form isolated and isolated data silos, so that it is difficult for credit information to fully realize its shared value.

Besides, benefiting from many mature cryptography techniques, the credit data is encrypted, or the design of double-zoned blockchain is adopted directly to ensure the security of credit data of users and ensure the absolute safety of credit data in the block chain. In this way, personal credit information can be traded directly on the blockchain, so our transaction data can be completely stored in the blockchain in the future and become our personal credit. All generated transactional big data will become clear to everyone Credit resources. More than that, the blockchain also collects and shares data openly and transparently among people. In this way, the "all" personal data scattered in the private sector and the public sector can be fully aggregated, taken from the users and used by users, and the open sharing of data and social interconnection can be promoted.

2. AdvancedCreditChain product overview

2.1 AdvancedCreditChain business briefing

In the Advanced credit chain system (referred to as ACDC system), each user can save the core data in their own internal chain, a small amount of summary index information provided to CreditChain's public blockchain. Users with query requests are forwarded through the CreditChain public blockchain to the original data provider (another user) for querying, so that each user can both query vast amounts of data without worrying about revealing his or her own business data. Each query is considered a transaction and broadcast to the entire chain. CreditChain uses a feature that cannot be tampered with by blockchain to build a viable technical framework.

- Does not share the original data while multi-party data sharing, enlarge data value.
- Data is valid and can not be tampered with.
- Instead of providing data passively, sigma participants take the initiative to participate.
- The company to be queried can get partial revenue.
- The newer the more valuable the data is.
- Provides data support for credit investigation and risk prevention.

2.2 AdvancedCreditChain credit information system function introduction

2.2.1 Unified data sharing registration rules

It is often more practical to collect the required data using more direct forms of cooperation, to agree on the necessary packages and classification and labeling, and to prepare the jointly submitted data. This may involve a joint review of all readily available data, including publicly available data. This more complete communication allows participants to decide on the classification and data and agree on them. ACDC therefore works in parallel on existing information (including publicly available data) and the identification of data requirements, generation of new information, and joint registration.

2.2.2 Blockchain public key encryption ensures data reliability

Public-key cryptography, also known as asymmetric cryptography, is an algorithm of cryptography that requires two keys, one a public key and the other a private key; one for encryption, and the other for decryption. The ciphertext obtained by using one of the keys to encrypt plaintext can only be decrypted with the corresponding other key to obtain the original plaintext; even the key originally used for encryption cannot be used for decryption. The use of this technology in the blockchain can further secure the data itself.

2.2.3 Provide free data inquiry

After the system database is set up, any organization and third-party companies can choose to query other people's requests. Querying any data in the system is for no reason, which means that any participating agency and business can see complete, open and transparent corporate credit data.

2.2.4 Shared transaction broadcast

Within ACDC, the entire chain is broadcasted on every transaction (modification) to ensure that the data can not be tampered with. Broadcasting is based on the existing blockchain model and uses distributed ledger storage. Optimized for point-to-point broadcast transmission, and trade-offs the amount of information and frequency in the propagation strategy.

2.2.5 Identify the authenticity of shared data through the whitelist system

Create a blacklist mechanism that exposes dishonest information throughout the chain. Blacklist dishonesty data is divided into public data, detailed information in two parts. Public data is part of the details of the data. It is an effective way to supervise and standardize the corporate credit system by publishing the list of disloyal clients analogous to the court system.

2.2.6 Introduced a complete set of mature credit rating system

ACDC introduced a professional credit rating team and a complete credit rating system. Customize and optimize for this product-specific business model. Emphasis will be given to highlighting the parts of the system that have a large impact on the value of the credit reference system, and

deleting the complicated and inefficient evaluation contents and system methods directly. In ensuring efficiency, but also ensure the accuracy of the data.

2.3 AdvancedCreditChain credit reference system features

♦ Decentralization: Single point storage of raw data, blockchain ledger sharing of summary information.

♦ Coin Day Destroy: The Coin Day Destroy equals the amount (in money) of each transaction multiplied by the time (days) accumulated since the transaction was last traded.

♦ Data Trading Authorization: Establish a complete and fair data trading authorization model.

♦ Smart Contract: Propose a unique new smart contract model.

♦ Public key encryption: Encrypt data Submit a copy to the blockchain to ensure that the data cannot be tampered with.

♦ Private Key Decryption: The user authorizes the query operation through the private key.

♦ Unalterable: every inquiry and update are regarded as an irreversible transaction, transaction broadcasting to the whole chain.

♦ Free data inquiry: Query users are free for charge, been queried user gets incomes.

♦ Accurate mechanism: provide margin mechanism to improve data accuracy.

♦ Arbitration Mechanism: Start the arbitration proceedings when there is an objection.

♦ Open Interface (API): The main data query interface is fully open to the public, making the system more convenient and quick to be applied to other social and information platforms.

3. Decentralize

Traditional data center alliance mode is generally a number of small data centers attached to a large data center, small data centers and large data centers for data interchange. This model of small data centers cannot trust each other, all the data through large data center exchange. The net result is that large data centers place the blockchain as a decentralized distributed data storage technology. Its core value is to create a safe and trustworthy system that allows organizations or individuals that are not trusted to interact with each other and trust each other's information and data without the coordination of an authority center. At the same time, the blockchain has realized the data cannot be tampered with and cannot be deleted through the techniques of cryptography, distributed agreement, consensus agreement and peer-to-peer network communication. Decentralization is a phenomenon or structure that can only occur in systems with many users or nodes, each connected to and affecting the other nodes, in other words, everyone is the center, and everyone Can all connect and influence other nodes. This phenomenon of flattening, opening-source and equalization or structure is called decentralization.

Centralized   Decentralized   Distributed
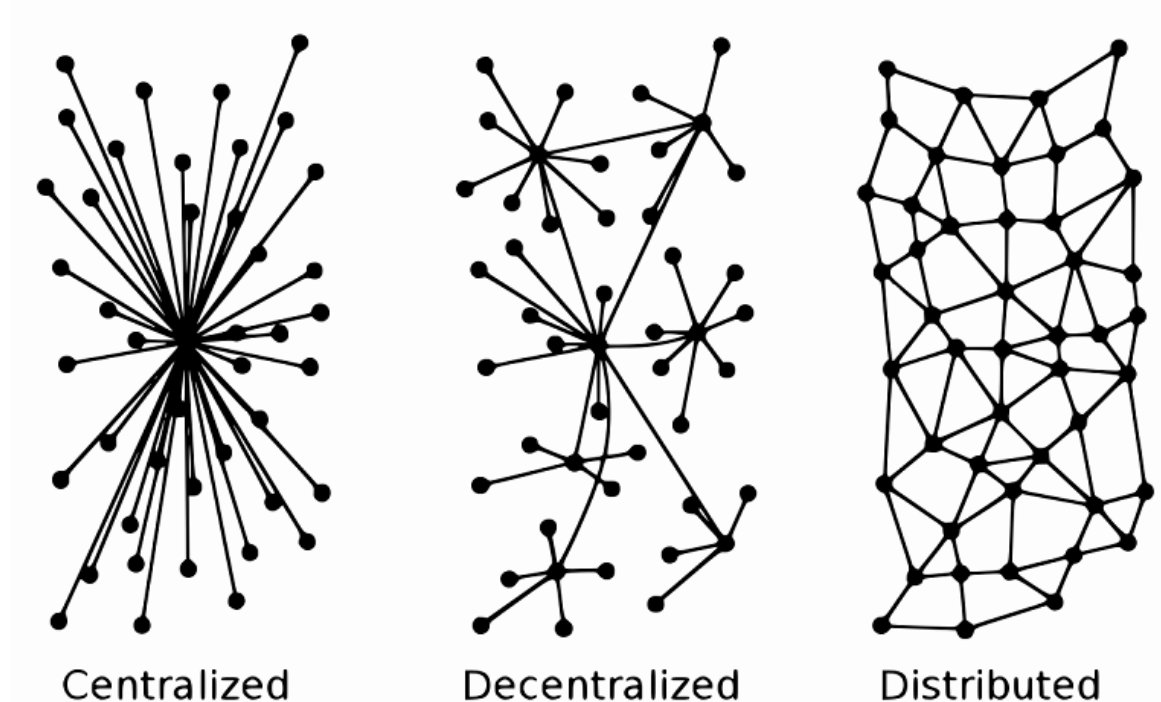
At the same time, "decentralization" is one of the typical characteristics of the blockchain, which uses the distributed storage and computing power, the rights and obligations of the entire network node are the same, and the data essence in the system is jointly maintained by the nodes of the entire network, so that the blockchain is not Then rely on the central processing node to achieve the distributed data storage, recording and updating. Each blockchain follows a uniform rule that is based on a cryptographic algorithm rather than a credit certificate, and the data update process requires user approval, thus establishing a blockchain that does not require intermediaries and trust agencies

Blockchain had been developed to solve a core problem, the issue of trust, from a variety of data, such as the supply chain finance pledge business, it will involve financial institutions, enterprises, warehousing, service providers, warehousing regulatory party There may be buyers and sellers on the five parties, including the business side. In this case, it is relatively troublesome to get back and forth between data. Because each of them has a way to record information, it is very complicated for the five users to reconcile together.

Industries also have upstream and downstream relations, such as raw materials and chemicals, and cosmetic products brands, automotive OEMs and auto parts industry is an upstream and downstream, which will also have the relevant vertical coordination. A better way is to record the

distributed ledgers to the blockchain each and everybody finally has a consensus that can be reached. Therefore, what the blockchain solves is how supply chain finance achieves a trusting relationship in a non-trusting system.

Traditional Supply Chain Finance As a result of a series of problems such as communication between core enterprises, high operating costs and complicated post-loan management, the result is that it takes a great deal of energy but cannot generate a reasonable return. The development of financial technology will truly change the traditional supply chain finance, not just simple on-lining, but also to promote supply chain finance more automated and intelligent through technology such as credit transaction, big data and blockchain, and create more value for the real economy.

Credit on the blockchain is based only on the direct data itself, the transactional data, without the need to synthesize information of different dimensions. Because blockchain deals with time arrows, the marginal cost of duplicated spending is no longer equal to zero, but directly proportional to the Coin Days Destroyed.

4. Coin Days Destroyed

Coin days destroyed is a very important concept of the blockchain. As the name implies, coin days destroyed is equal to the amount (in money) of each transaction multiplied by the time (days) it accumulated from the last exchange, for example, if a user spends 10 digital currencies received 100 days ago, coin days destroyed is 1000 currency days.

The coin days destroyed as a weight factor for the credit rating of blockchain transactions can prevent brush customers from repeatedly transferring funds between two accounts for brushing credit, and can prevent bad judges from making a large number of small transactions with malicious negative feedback. This is because in a transaction, the more coin days destroyed, the higher the weight of credit rating. The rating of the first transaction is valid when the brush customer attempts to give a favorable comment on repeated transactions with two accounts. However, the accumulated coin days in history have been destroyed when the transaction is completed. When the second transaction is conducted, Due to the very small accumulation of coin days immediately after the first transaction, correspondingly, the contribution to the credit rating is minimal, and the sum of the currency days destroyed in all the transactions is also very small. Users repeatedly use the same sum of money Their own brush praise, no matter how many times, the final effect of the first transaction with the credit rating is almost the same. Similarly, when a bad reviewer attempts to maliciously evaluate a user through a large number of small transactions, since the credit rating is directly proportional to the destruction of the coin day, the transaction amount is also too small to affect the user's credit almost equally.

4.1 Traditional credit evaluation model (cumulative model)

Accumulative model refers to the original credit points based on the direct addition and subtraction, the model is as follows:

$$R_n = R_{n-1} + r_n$$
$$r_n \in \{-1,0,1\}$$

Rn and Rn-1 denote the credit scores obtained by the blockchain users respectively after the nth and n-1th transactions,

$$r_n \in \{-1, 0, 1\}$$

That is, {detractor, passive, promoter}, that is, when the "detractor" in the original credit points on the basis of plus "-1" points, when users get in the passive is based on the original credit points plus "0 "points, adding" +1 "points to the original credit points when the user gets promoter comments. This evaluation model can more intuitively show the credit score of the trader and is more convenient and simple to operate, providing a credit reference for both parties to a certain extent. However, due to the fact that the amount of transaction is not taken into account, users are flooded with credit scams and other factors such as the blockchain timestamp are not taken into consideration. As a result, the marginal cost of the transaction is close to zero, and the scrubber can create a large number of false transactions in a short period of time. Honest traders cannot compete in a fair-trading environment. Due to the ubiquity of the two behavioral patterns of fake credit and fake discrepancy assessment, this model hardly reflects the true credit of block traders.

4.2 Weight Model Based on the Coin days destroyed

Weight model refers to the user credit rating obtained by the credit multiplied by the transaction coin days destroyed and then obtain the user's final credit value, the model is as follows:
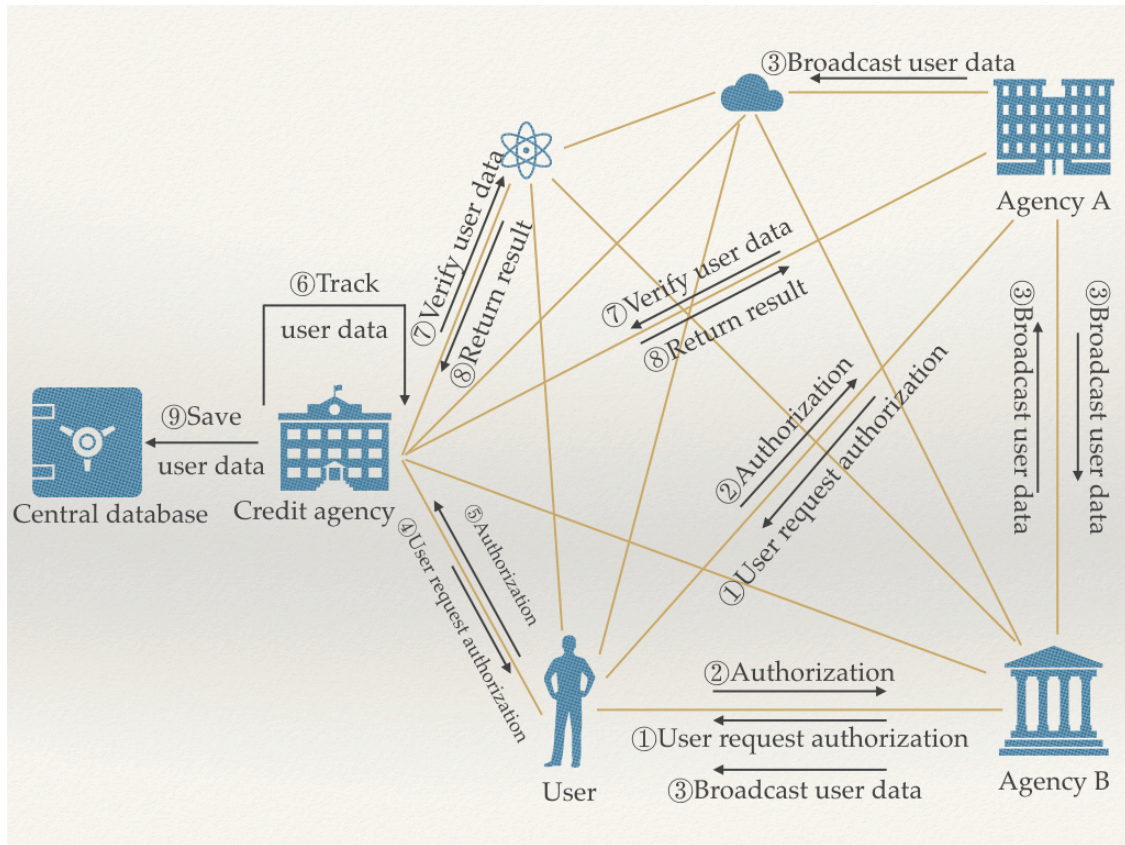
$$R_n = \sum_{i=1}^{i=n} R_i * W_i$$

$$W_i = C_i * D_i$$

$$R_i \in \{-1, 0, 1\}$$

$$i, W_i, C_i, D_i \in (0, +\infty)$$

R_n represents the user's credit score, R_i is the credit value of the user in the i-th transaction, W_i is the coin days destroyed in the i-th transaction, C_i is the i-th transaction amount, D_i is the i-th transaction distance the time accumulated in the last exchange.

5. Credit information transaction authorization introduction

①Other agencies A, B to the user request authorization, ② after the user's license, ③ the various aspects of the user's data broadcast to the blockchain, the chain of these data only shows the address of the user Attribute, and will not disclose user privacy. ④ The credit institution requests authorization from user, ⑤ After the authorization of user, it tracks⑥ the data in its own node and learns the past credit history, repayment records, overdue records and current general debt situation of user. ⑦ ⑧ credit agencies in the blockchain to verify the authenticity of the data,

⑨ stored in the central database, and then analyze their credit judgment. In this mode, credit data can be cross-verified by multiple sources, so the authenticity of the data is guaranteed and cannot be tampered with by enterprises or individuals.

In this model, institutions and users (companies) are all involved in the evaluation to the maximum extent. The main features of the model are two: a good weight and multiple validation. In this model, different agencies and enterprises have been well weighted, greatly weakened the imbalance of the credit system caused by "head effect", and realized the authorization and verification model that "the strong are not overbearing and the weak are not shrinking." . And credit data in this model can be multi-source cross-validated. We can see that the sending of either party's data will be verified and authorized by the third or even the fourth party, so the authenticity of the data is guaranteed and cannot be tampered with by enterprises or individuals.

6 Smart contracts

6.1 Contract type

In lieu of unspent outputs of Bitcoin, ACDC uses stateful accounts. When those accounts specify executable code, they are known more generally as contracts. Since an account is a type of contract (one with no executable code), we refer to both as" contracts" in full generality.

Each contract has a "manager", which in the case of an account is simply the owner. If the contract is agged as spendable, the manager may spend the funds associated with the contract. In addition, each contract may specify the hash of a public key used to sign or mine blocks in the proof-of-stake protocol. The private key may or may not be controlled by the manager.

Formally, a contract is represented as:

type contract = {

counter: int; (* counter to prevent repeat attacks *)

manager: id; (* hash of the contract's manager public key *) balance: Int64.t; (* balance held *)

signer: id option; (* id of the signer *)

code: opcode list; (* contract code as a list of opcodes *) storage: data list; (* storage of the contract *)

spendable: bool; (* may the money be spent by the manager? *) delegatable: bool; (* may the manager change the signing key? *)

}

The handle of a contract is the hash of its initial content. Attempting to create a contract whose hash would collide with an existing contract is an invalid operation and cannot be included in a valid block.

Note that data is represented as the union type.

type data =

| STRING of string | INT of int

where INT is a signed 64-bit integer and string is an array of up to 1024 bytes. The storage capacity is limited to 16 384 bytes, counting the integers as eight bytes and the strings as their length.

6.2 Origination

The origination operation may be used to create a new contract, it species the code of the contract and the initial content of the contract's storage. If the handle is already the handle of an existing contract, the origination is rejected (there is no reason for this to ever happen, unless by mistake or malice).

A contract needs a minimum balance of 1 to remain active. If the balance falls below this number, the contract is destroyed.

6.3 Transactions

A transaction is a message sent from one contract to another contract, this message is represented as:

type transaction = {

amount: amount; (* amount being sent *)

parameters: data list; (* parameters passed to the script *) (* counter (invoice id) to avoid repeat attacks *)

counter: int;

destination: contract hash;

}

Such a transaction can be sent from a contract if signed using the manager's key or can be sent programmatically by code executing in the contract. When the transaction is received, the amount is added to the destination contract's balance and the destination contract's code is executed. This code can make use of the parameters passed to it, it can read and write the contract's storage, change the signature key and post transactions to other contracts.

The role of the counter is to prevent replay attacks. A transaction is only valid if the contract's counter is equal to the transaction's counter. Once a transaction is applied, the counter increases by one, preventing the transaction from being reused.

The transaction also includes the block hash of a recent block that the client considers valid. If an attacker ever succeeds in forcing a long reorganization with a fork, he will be unable to include such transactions, making the fork obviously fake. This is a last line of defense, TAPOS is a great system to prevent long reorganizations but not a very good system to prevent short term double spending.

The pair (account_handle, counter) is roughly the equivalent of an unspent output in Bitcoin.

6.4 Storage fees

Since storage imposes a major cost on the network, a minimum fee of 1 ACDC is assessed for each byte increase in the storage. For instance, if after the execution of a transaction, an integer has been added to the storage and ten characters have been appended to an existing string in the storage, then 18 ACDC will be withdrawn from the contract's balance and destroyed.

6.5 Code

The language is stack based, with high level data types and primitives and strict static type checking. Its design is inspired by Forth, Scheme, ML and Cat. A full specification of the instruction set is available in. This specification gives the complete instruction set, type system and semantics of the language. It is meant as a precise reference manual, not an easy introduction.

6.6 Transaction fee

So far, this system is similar to the way Ethereum handles transaction. However, we differ in the way we handle fees. Ethereum allows arbitrarily long programs to execute by requiring a fee that increases linearly with the program's executing time. Unfortunately, while this does provide an incentive for one miner to verify the transaction, it does not provide such an incentive to other miners, who must also verify this transaction. In practice, most of the interesting pro- grams that can be used for smart contracts are very short. Thus, we simplify the construction by imposing a hard cap on the number of steps we allow the programs to run for.

If the hard cap proves too tight for some programs, they can break the execution in multiple steps and use multiple transactions to execute fully. Since Tezos is amendable, this cap can be changed in the future, or advanced primitives can be introduced as new opcodes.

If the account permits, the signature key may be changed by issuing a signed message requesting the change.

7. AdvancedCreditChain business advantages and development planning

7.1 Analysis of Porter Competitive Advantage of ACDC

According to the Michael Porter's Five Forces Model, a five-pronged competitive analysis model proposed by Michael Porter in the early 1980s, we conducted an in-depth analysis of ACDC. The five major forces that have an impact on competitiveness are the competitors, buyers, suppliers and replacers, respectively, which have the major influence on ACDC, competitors and replacements.

In the enterprise credit investigation, more competitors came from the traditional enterprise credit intermediary institutions, but the data were lack of sharing, the credit institution and the user information were not symmetrical, there was no effective sharing and cooperation between the agencies, and the agencies were isolated from each other Information, resulting in serious information island issues, coupled with institutional mechanisms and the credit information technology industry architecture issues, resulting in the traditional credit information agencies have mastered the massive credit information has been unable to truly and efficiently use. In addition, due to the fierce competition between traditional credit reporting companies, in the face of

customers' desire for rating of "AAA", credit rating companies inevitably face moral hazard and deliberately or unintentionally ignore some potential factors to give customers Satisfactory rating. Mr. Rayloard, my team consultant, downgraded the rating given by some rating agencies to actual corporate bond issuance and there are numerous examples of such cases being traceable in China Investment Bank's real business. Compared with competitors in the industry, ACDC's credit information system interacts with each other through blockchain technology with secure encryption through the decentralization of mutual trust between trusted agencies and individuals without the authority of central agencies. Combined with the means of destruction of the currency days, credit transaction costs given to accurately reflect the true customer credit, from math to solve the impact of cheating means on credit.

In today's blockchain industry, new concepts are threatened by new entrants with similar capabilities shortly after they are proposed, so we designed the perfect data sharing rules from the beginning of designing ACDC, a reliable public key Encrypted, gratuitous data inquiries, shared data broadcasts, real blacklists that can be shared and efficient and mature credit rating system. Have a higher technical barriers, alternative to want to achieve the replacement of ACDC is theoretically possible, but need to pay the high cost of time and research and development costs, plus ACDC's native attributes - support for metadata upgrades, self-evolving code evolution Protocol can absorb the advantages of any kind of blockchain-based credit information system and realize all kinds of operations on its regular blockchain by means of simple functional modules, so that the functional optimization of the substitutes not only does not threaten the ACDC , But will continue to promote ACDC function upgrades, to achieve a kind of "little power" effect in ancient Chinese martial arts literature.

Obviously, ACDC, with its full-featured, technical and pain-solving points, not only has less adverse impact on its competitors but also its evolutionary upgrade, so ACDC has a unique And can not ignore the competitiveness.

7.2 ACDC resource advantage analysis

In 1997, Teece (1997) and other scholars put forward the theory of motivation, that resources can be divided into four levels:

The first level is the public knowledge gained. The ACDC Cryptographic Credit System handles network layer tasks through a cyber shell by applying cryptography to the field of information.

The second layer is a proprietary asset, such as trade secrets, production tips and special functions, which are very difficult to copy and imitate because of the incorporation of intangible knowledge in the enterprise. ACDC through the team's hard research and development, with reliable sharing rules, encryption technology and gratuitous blacklist inquiries, set up a unique credit rating system and technical barriers.

The third layer is the management team's ability and external resources, that is, the production factors and proprietary assets organically integrated organizational practices and management activities, for those who have a significant advantage over competitors is the main source of competitive advantage. The famous "Pan Rose effect." Penrose, 1959 argues that the scale can not be compared in terms of size, the key depends on the knowledge and management capabilities of business managers. Although the current market size of ACDC is still in its infancy, our team has consultants A and B Consultant skills, highlighting the relevant research and development under the strength of the line) with excellent management capabilities, ACDC will be the latter part of the development to bring continuous power.

The fourth level is motivation, emphasizing that in order to adapt to the changing external environment, we must continuously acquire and integrate internal and external social organizations and create proprietary assets such as proprietary technology assets, prestige assets and market assets through the capacity of resource integration. ACDC team in addition to R & D technology has a very high standard, there are outstanding achievements in the prestige. At present, the team has close cooperation and contacts with the government of Vietnam, the government of Benin and traditional credit reporting enterprises. In fact, ACDC has reached initial agreement with the Vietnamese government and the government of Benin. Hồ Tri Liêm, commander-in-chief of the Vietnam Communications Corps and manager of Vietnam Army Football Team, showed his appreciation of the ACDC project philosophy. Mr. Patrice Talon, President of Benin, also expressed his strong interest in ACDC and said that it would provide the necessary assistance to the ACDC project. In the meantime, the ACDC team is also actively negotiating with relevant departments in Singapore, Japan, Italy, Lesotho and other countries to bring a new credit information system and solve the existing pain points.

Based on an in-depth analysis of ACDC's four-layer power capability, we can see that ACDC has a great potential to enhance its resources. This advantage will be accelerated when its popularity and influence are expanded.

7.3 Development Plan

Although ACDC has distinctive features and outstanding advantages compared with traditional credit information industry, ACDC is a brand-new system after all. As the centralization of ACDC will certainly touch the interests of the traditional credit rating agencies, it will inevitably hinder the implementation of ACDC. However, competition that ACDC brought to the industry is not destructive, but to promote improvement. After effective communication, the team believes that it can consolidate the elites both inside and outside of the industry and with the coordination of governments. The ACDC team has strong confidence to push the project smoothly and create a transparent and healthy business environment for ACDC countries. Social development and stability are paramount to fairness and justice. Team ACDC is currently working with a leading financial technology company in China and will use its current financial information, rating history and share price performance data of 17,000 credit entities currently in China in the future.

With ACDC this will be easier to achieve, which is also a concern for a number of state leaders highly optimistic about the ACDC is an important factor. In the future, ACDC will work closely with risk control companies, headhunters, accounting and auditing firms, and background research firms to systematize traditional credit reporting and plug in wing of Blockchain technology for the credit reference industry.

8. Reference

. [1] Vitalik Buterin. Slasher: A punitive proof-of-stake algorithm. https://blog.ethereum.org/2014/01/15/ slasher-a-punitive-proof-of-stake-algorithm/, 2014.

. [2] Ariel Gabizon Iddo Bentov and Alex Mizrahi. Cryptocurrencies without proof of work. http://www.cs.technion.ac.il/~idddo/CoA.pdf, 2014.

. [3] Peter Suber. Nomic: A game of self-amendment. http://legacy.earlham.edu/~peters/writing/nomic.htm, 1982.

. [4] Jérôme Vouillon. Lwt: a cooperative thread library. 2008.

. [5] Tezos project. Formal specification of the tezos smart contract language. https://tezos.com/pages/tech.html, 2014.

. [6] Lending Relationships and Credit Rationing: The Impact of Securitization. Santiago Carbovalverde, Hans Degryse, Francisco Rodriguezfernandez

. [7] Bitcoin and the Blockchain: a coup d'état in Digital Heterotopia? Donncha Kavanagh, Gianluca Miscione

. [8] Collaborative Filtering on the Blockchain: A Secure Recommender System for e-Commerce. Remo Manuel Frey, Dominic Worner, Alexander Ilic

. [9] An Analysis of the Cryptocurrency Industry. Ryan Farell

. [10] Blockchain Demonstration Shows Potential Loan Market Improvements. Credit Suisse

. [11] Integrating blockchain and artificial intelligence into the accounting curriculum. Sean Stein Smith