浙江大学

Team-Project ReportBlock chain and Smart Contract

Group Number: 1

ID	Member
3180103772	张溢弛
3180103162	张琦
3180103164	袁浩然
3180103485	王晨露
3180103501	聂俊哲
3180103771	求昊泽
3180103809	朱王逸
3180103852	季奕君
3180105501	康大凯
3180105099	康锦辉

前言

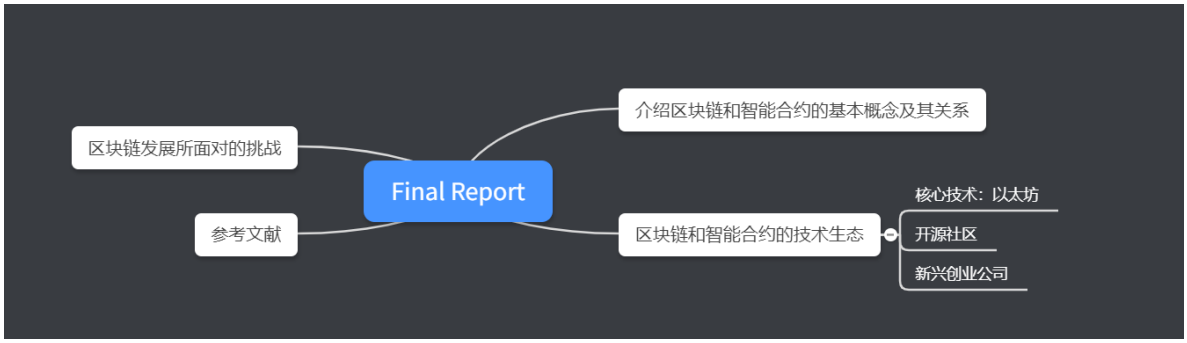
这是浙江大学2020年春学期信息安全原理第一大组的课程项目的Final Report，我们小组研究的课题是“Block Chain and Smart Contract”， 即《区块链和智能合约》，我们小组成员广泛搜集资料和查阅文献，将结果整理成了一个这份报告和展示PPT,然而区块链和智能合约相关的项目开发基本上达到了企业级项目的开发层次和要求，因此在实践操作部分我们小组只能尝试编写一些比较简单和基本的只能合约作为，真正的工业级开发需要等到后续知识的深入学习之后在进行实践操作。

本最终报告共分为如下几个部分：第一部分主要介绍了区块链技术和智能合约技术的一些基本概念和它们之间的关系，并介绍了公有链，私有链，联盟链等概念；第二部分主要介绍区块链和智能合约技术的技术生态，包括核心技术以太坊，开源社区(以GitHub为代表)中的一些开源项目和区块链系得创业企业对区块链和智能合约技术的发展和促进；第三部分则主要介绍了区块链和智能合约技术在发展的过程中遇到的技术瓶颈和未来的发展方向，最后第一部分则是我们在撰写报告的过程中参考的一些文献和网站。

考虑到《信息安全原理》作为一门双语课的要求，报告的正文部分我们统一采用英文写成。报告的结构如下图所示。

第一大组全体成员

2020.04.12



Content

Chapter 1：Introduction to BlockChain and Smart Contract

1.0 Background

Nowadays，the block chain and smart contract are becoming more and more popular in open-source community and business because of its safety and reliability. In our team project of principles of information security, we will focus on the topic of block chain and smart contract.

1.1 Introduction to blockchain

Blockchain technology is considered to be the **core driving force** of the third revolution of the Internet and the next generation of disruptive technology. Blockchain technology provides a new way to record and communicate value which can make value transmission more transparent fair and secure and realize the transformation from data interconnection to value interconnection to order interconnection. It will probably revolutionize the way in which the value of human society as a whole is transmitted.

Block chain can be divided into public chain, private chain, alliance chain and other types.

1.1.1 The development of block chain

The initial concept of blockchain first appeared in the early 1990s. In 1991, Stuart Haber and Scott Stornetta described the first data block application based on cryptography to implement a distributed file system with document timestamps to prevent tampering, forgery and denial. In 1992, Bayer, Haber, and Stornetta incorporated the Merkle tree into the design to improve the efficiency of data recording by forming multiple document certificates into a single block.

With the development and popularization of Internet technology, it was not until 2008 that Satoshi Nakamoto realized the first example based on the above ideas and published A white paper titled “Bitcoin: A Peer to Peer Electronic Cash System”. The paper proposes an electronic cash mechanism that relies on cryptography technology and calculation methods to realize the same as paper cash, which is the core of the later blockchain technology. In this way, anyone can conduct transactions without knowing the background information of the other party, and no third party is required to intervene. In November 2008, Satoshi Nakamoto registered the Bitcoin project at “Sourceforge.org”, and on Jan. 3, 2009, a Bitcoin block with the serial number 0, or genesis block, appeared in Finland. On January 9, 2009, the bitcoin block with the serial number of 1 was excavated in order. The block was linked with the serial number of creation block with the serial number of 0 in a chronological order to form a chain, which marked the birth of an instantiated digital currency block chain.

In fact, bitcoin can be seen as a classic example of blockchain technology. Block chain provides new ways to record and communicate value, can let value delivery become more transparent and democratic, efficient, safe and decentralization. Therefore, block chain may use technology to build trust and trust throughout the entire pass, thus providing a truly subverts the traditional value of the human society the new way.

1.1.2 block chain technology and contract theory

Block chain technology is an integrated application of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other technologies. It is a distributed ledger formed by using cryptography technology to add blocks confirmed by consensus in order. In addition to the well-known characteristics of decentralization and de-trust, information transparency, identity anonymity, traceability and collective maintenance, Contract Theory plays an important role in the block chain technology system. The table below shows the framework of block chain 3.0.

The application layer	Dapp application
The contract layer	Intelligent contract, The virtual machine
The incentive layer	Release mechanism, Allocation mechanism
The consensus layer	PBFT, PoS, PoW, DPoS
The network layer	P2P network, Transmission mechanism
The data layer	Merkle Tree, digital signature, Asymmetric encryption algorithm

(Table: the framework of block chain 3.0)

On October 10, 2016, the 2016 Nobel Prize in economics was awarded to Oliver Hart of Harvard University and Bengt Holmstrom of the Massachusetts institute of technology for their contributions to contract theory. This theory mainly studies how to design the optimal contract under the condition of information asymmetry and finally achieve the global optimal. In the decentralized market of blockchain, there are two markets: one is the resource transaction market with blockchain as the accounting book, recording the system (electronic cash, real estate, enterprise operating system, etc.); The other is the blockchain bookkeeping service trading market where miners compete for bookkeeping rights to get fees under the constraint of the consensus mechanism. The intrinsic relationship between these two market behaviors and the two markets is reflected in the relationship between fees and the market value of system resources. Decentralization means peer-to-peer equality for all parties involved in a transaction. From the perspective of contract theory, the consensus mechanism is a contract arrangement that

restricts the participation of all parties in the decentralized market of blockchain. Consensus mechanism solves the problem of mutual trust among nodes under the idea of decentralization and is the core rule that restricts the cost input and income distribution among nodes. The new peer-to-peer and seemingly loose trading environment of contracts-constrained blockchain can reduce transaction costs in a competitive environment by arranging contracts without centralized institutions, such as communication, competition for customers, and waste of time caused by coordination and distribution.

Therefore, the blockchain is viewed from the perspective of contract, which is the reason why the decentralized, point-to-point blockchain market can still operate normally without the existence of centralized companies.

1.1.3 A Simple Conclusion

While traditional Internet focuses on the exchange of information, blockchain focuses on the exchange of value. In the era of Internet popularization, people not only exchange information through the network, but also exchange, trade and transfer the value of some digital assets, and even sign some contracts directly on the network. Blockchain delivers value through smart contracts and ownership of information. The information transmitted in the network can be copied and pasted at will, while the block chain data sovereignty technology realizes the value transfer of assets by attaching ownership tags to each information to identify the ownership. Any technology is a means, not an end, and we must not forget our original intention in order to use it. The same is true of block chain technology. On the basis of fully analyzing the social status and industry background, we should study the application mode of block chain in all walks of life.

1.2 Introduction to Smart Contract

1.2.1 Definition

Traditional contract

For a traditional contract, the execution of it requires human validation to check the terms and conditions and decide the next steps according to the written agreement. Therefore, a traditional contract can be:

- Time-consuming — checking the contract, validation, and approval, enabling next steps, etc.
- Resource consuming — execution of a traditional contract may require human intervention
- Costly — it may involve a third party; this is even true during a dispute.

The more complex the contract is, the more it requires control and the more there is a risk of disputes. For example, this can involve several execution steps that enable specific actions or that give rise to certain privileges.

There is another way to deal with a contract in a way that it overcomes these challenges and limitations mentioned previously. As technology evolves, the way we deal with contracts evolve, and the smart contract is born. However, what is a smart contract?

Smart contract

Smart contracts are translations of an agreement, including terms and conditions into a computational code (script). Blockchain developers write the script in a programming language like Java, C++, etc. in a way that it is void of ambiguity and does not lead to misinterpretation. The code translates a set of rules that are automatically executed and validated. A straightforward example is a translation of: "if X provides the service, Y pays for it."

Smart contracts' code is uploaded into the blockchain to check the validity of a contract and enable required steps. From its initialization, a smart contract is automatically executed. The main difference between a smart contract and a traditional contract is that a smart contract doesn't rely on a third party; cryptographic code enforces it.

We can consider a vending machine that is implementing a smart contract mechanically. It verifies the following properties:

- There is **no third-party** involved in the transaction.
- When you put your coin into the machine and select your product, it delivers the product directly to you, as long as you meet the terms and conditions — your coin has the same or higher value than the product you want to purchase.

  Now that we have more understanding of what smart contracts are, let's see how smart contract works.

1.2.2 Development of smart contract

Smart contracts were first proposed in the early 1990s by computer scientist, lawyer and cryptographer Nick Szabo, who coined the term. With the present implementations, based on blockchains, "smart contract" is mostly used more specifically in the sense of general purpose computation that takes place on a blockchain or distributed ledger. In this interpretation, used for example by the Ethereum Foundation or IBM, a smart contract is not necessarily related to the classical concept of a contract, but can be any kind of computer program.

A smart contract also can be regarded as a secured stored procedure as its execution and codified effects like the transfer of some value between parties are strictly enforced and can not be manipulated, after a transaction with specific contract details is stored into a blockchain or distributed ledger. That's because the actual execution of contracts is controlled and audited by the platform, not by any arbitrary server-side programs connecting to the platform.

In 2018, a US Senate report said: "While smart contracts might sound new, the concept is rooted in basic contract law. Usually, the judicial system adjudicates contractual disputes and enforces terms, but it is also common to have another arbitration method, especially for international transactions. With smart contracts, a program enforces the contract built into the code."

By implementing the Decree on Development of Digital Economy, Belarus has become the first-ever country to legalize smart contracts. Belarusian lawyer Denis Aleinikov is considered to be the author of a smart contract legal concept introduced by the decree.

1.2.3 Security issues

A smart contract is "a computerized transaction protocol that executes the terms of a contract". A blockchain-based smart contract is visible to all users of said blockchain. However, this leads to a situation where bugs, including security holes, are visible to all yet may not be quickly fixed.

Such an attack, difficult to fix quickly, was successfully executed on The DAO in June 2016, draining US$50 million in Ether while developers attempted to come to a solution that would gain consensus. The DAO program had a time delay in place before the hacker could remove the funds; a hard fork of the Ethereum software was done to claw back the funds from the attacker before the time limit expired.

Issues in Ethereum smart contracts, in particular, include ambiguities and easy-but-insecure constructs in its contract language Solidity, compiler bugs, Ethereum Virtual Machine bugs, attacks on the blockchain network, the immutability of bugs and that there is no central source documenting known vulnerabilities, attacks and problematic constructs.

1.2.4 Advantages of smart contract

- **Decentralization :** No need to rely on the participation or intervention of the third party central organization, the supervision and arbitration of the contract are completed by computer programs.
- **Efficiency :** Smart contract reduces the intermediate links, can respond to requests at any time, and greatly improves the execution efficiency.
- **Low-cost :** Based on computer programs, controlled by preset codes, once the contract is broken, the code will be enforced, reducing the cost of adjudication, execution and supervision of the contract.
- **Accuracy :** Smart contract is controlled by computer programs without human's participation, so as to eliminate the possibility of mistakes and improve the accuracy of smart contract.
- **Tamper-refused :** After the smart contract is deployed, all contents cannot be modified, and neither party can interfere with the contract.

1.2.5 Relations between block chain and smart contract

Till now, there are already two generations of blockchain technology. Cryptocurrencies have emerged as the first generation of blockchain technology. Cryptocurrencies are basically digital currencies that are based on cryptographic techniques and peer-to-peer network. The first and most popular example of cryptocurrencies is Bitcoin. Other blockchains such as Ethereum have emerged as the second generation of blockchain to allow building complex distributed applications beyond the cryptocurrencies. And smart contracts are considered as the main element of this generation where Ethereum blockchain is the most popular blockchain for developing smart contracts. Ethereum is a public blockchain with a built-in Turing-complete language to allow writing any smart contract and decentralized application.

A smart contract has an account balance, a private storage and executable code. The contract’s state comprises the storage and the balance of the contract. The state is stored on the blockchain and it is updated each time the contract is invoked. Once the contract is deployed into the blockchain, the contract code cannot be changed. To run a contract, users can simply send a transaction to the contract’s address. This transaction will then be executed by every consensus node in the network to reach a consensus on its output. The contract’s state will then be updated accordingly. The contract can, based on the transaction it receives, read/write to its private storage, store money into its account balance,

send/receive messages or money from users/other contracts or even create new contracts.

In conclusion, blockchain technology is a distributed database that records all transactions that have ever occurred in the network. The main feature of blockchain is that it allows untrusted parties to communicate between each other without the need of a trusted third party. Different distributed applications beyond cryptocurrencies can be deployed on top of blockchain. One of these applications is smart contracts, which are executable codes that facilitate, execute and enforce an agreement between untrusted parties. Ethereum is currently the most common blockchain platform for developing smart contracts, although there are some other available platforms. However, since there's no universally agreed definition of smart contracts, in theory, other techniques, some of which are even not blockchain technology, can also be adopted for developing smart contracts.

1.2.6 Possible usages

Smarts contracts can be applied and used in several industries. We can use a smart contract in many areas such as:

- Ensuring the authenticity of a copyrighted product — A smart contract helps ensure that the product a customer is buying is authentic and not just a perfect copy. It can be achieved since the information stored on blockchain is immutable making it easier, for instance, to prove that a given product belongs to a specific line of products.
- Money or currency transfer without an intermediary.
- Protect intellectual property.
- Protection from theft and counterfeit — tampering a block inside a blockchain requires tampering with all the previous blocks which will ultimately lead to tampering with the initial block which is impossible. Selling a good that does not have a transaction recorded in the blockchain will lead to a rejection.
- Internet of things — the idea here is to process transactions automatically, no matter how many parties are involved from end to end. For instance, from a vendor (A) to a buyer (B), the good may need to be transported by a transporter (T) and delivered to a different transporter. A smart contract can execute these steps automatically and quickly. When a specific action or condition is met, the next step is automatically enabled. A financial transaction can happen as much as needed.
- To authenticate certificates (job certificates, diplomas, etc.)
- Insurance — Like many other sectors, the insurance sector has explored the applicability of blockchain and started to implement smart contracts.

A smart contract has many advantages — it has made contract execution quicker, it can effectively reduce cost, and its application can go beyond its current use. Currently, there are many ideas businesses want to implement using the contract as they are growing in awareness of the advantages smart contract offers. A smart contract is not yet used to its full potential and our imagination and skills to implement the smart contract are limitless.

There is a growing number of blockchain enthusiasts. Smart contract's use will be broader, and more businesses will use it in the future. The first big step to achieve a flawless smart contract is to reach maturity.

Chapter 2： Ecology and development of Block chain and Smart Contract

According to our group research, we find a pretty good ecology of the block chain and smart contract industry, which includes many open-source projects on GitHub with many active developers and amount of small and medium sized startups whose core business is the development and application of blockchain platform in many fields, like trading of technological achievements and so on. Therefore, in this part of our report, we will introduce some famous open-source projects and startups in the blockchain.

2.1 Ethereum: a core technology

2.1.1 A simple Introduction

Like other blockchains, Ethereum has a native cryptocurrency called Ether (ETH). ETH is digital money. If you've heard of Bitcoin, ETH has many of the same features. It is purely digital, and can be sent to anyone anywhere in the world instantly. The supply of ETH isn't controlled by any government or company - it is decentralized, and it is scarce. People all over the world use ETH to make payments, as a store of value, or as collateral.

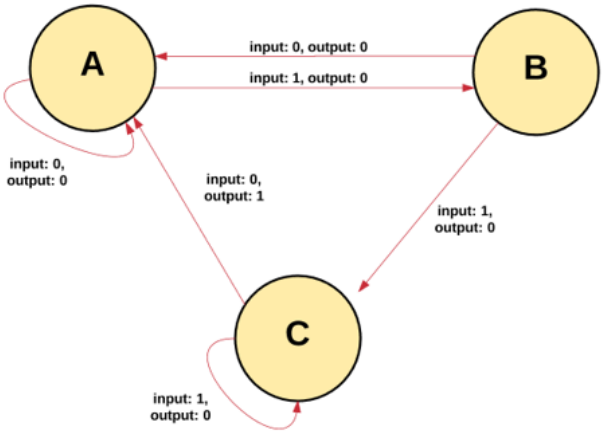
But unlike other blockchains, Ethereum can do much more. Ethereum is programmable, which means that developers can use it to build new kinds of applications. These decentralized applications gain the benefits of cryptocurrency and blockchain technology. They can be trustworthy, meaning that once they are "uploaded" to Ethereum, they will always run as programmed. They can control digital assets in order to create new kinds of financial applications. They can be decentralized, meaning that no single entity or person controls them.

Right now, thousands of developers all over the world are building applications on Ethereum, and inventing new kinds of applications, many of which you can use today:

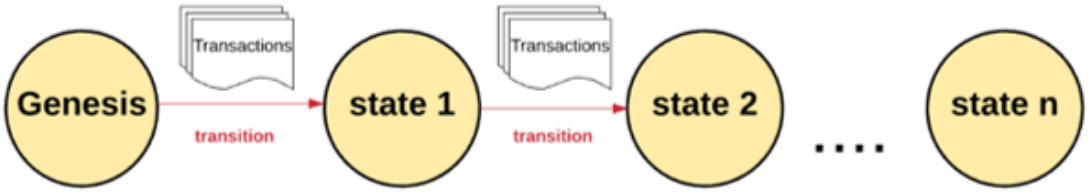
1. Cryptocurrency wallets that let you make cheap, instant payments with ETH or other assets
2. Financial applications that let you borrow, lend, or invest your digital assets
3. Decentralized markets, that let you trade digital assets, or even trade "predictions" about events in the real world
4. Games where you own in-game assets, and can even make real money

2.1.2 The paradigm of Ethereum blockchain

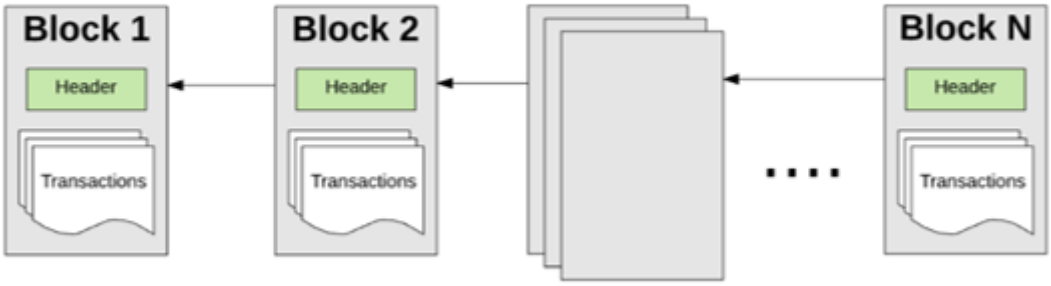
The Ethereum blockchain is essentially a transaction-based state machine. In computer science, a state machine refers to something that will read a series of inputs and, based on those inputs, will transition to a new state.



With Ethereum's state machine, we begin with a "genesis state." This is analogous to a blank slate, before any transactions have happened on the network. When transactions are executed, this genesis state transitions into some final state. At any point in time, this final state represents the current state of Ethereum.



The state of Ethereum has millions of transactions. These transactions are grouped into "blocks." A block contains a series of transactions, and each block is chained together with its previous block.



To cause a transition from one state to the next, a transaction must be valid. For a transaction to be considered valid, it must go through a validation process known as mining. Mining is when a group of nodes (i.e. computers) expend their compute resources to create a block of valid transactions.

Any node on the network that declares itself as a miner can attempt to create and validate a block. Lots of miners from around the world try to create and validate blocks at the same time. Each miner provides a mathematical "proof" when submitting a block to the blockchain, and this proof acts as a guarantee: if

the proof exists, the block must be valid.

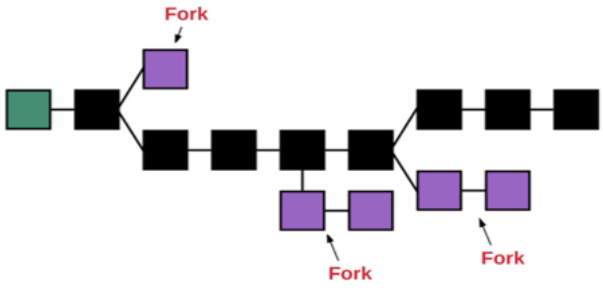
For a block to be added to the main blockchain, the miner must prove it faster than any other competitor miner. The process of validating each block by having a miner provide a mathematical proof is known as a "proof of work."

A miner who validates a new block is rewarded with a certain amount of value for doing this work. What is that value? The Ethereum blockchain uses an intrinsic digital token called "Ether." Every time a miner proves a block, new Ether tokens are generated and awarded.

But then we might wonder: what guarantees that everyone sticks to one chain of blocks? How can we be sure that there doesn't exist a subset of miners who will decide to create their own chain of blocks?

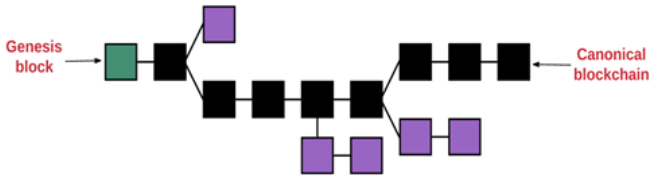
Earlier, we defined a blockchain as a transactional singleton machine with shared-state. Using this definition, we can understand the correct current state is a single global truth, which everyone must accept. Having multiple states (or chains) would ruin the whole system, because it would be impossible to agree on which state was the correct one. If the chains were to diverge, you might own 10 coins on one chain, 20 on another, and 40 on another. In this scenario, there would be no way to determine which chain was the most "valid."

Whenever multiple paths are generated, a "fork" occurs. We typically want to avoid forks, because they disrupt the system and force people to choose which chain they "believe" in.



To determine which path is most valid and prevent multiple chains, Ethereum uses a mechanism called the **"GHOST protocol."** , **"GHOST" = "Greedy Heaviest Observed Subtree"**

In simple terms, the GHOST protocol says we must pick the path that has had the most computation done upon it. One way to determine that path is to use the block number of the most recent block (the "leaf block"), which represents the total number of blocks in the current path (not counting the genesis block). The higher the block number, the longer the path and the greater the mining effort that must have gone into arriving at the leaf. Using this reasoning allows us to agree on the canonical version of the current state.

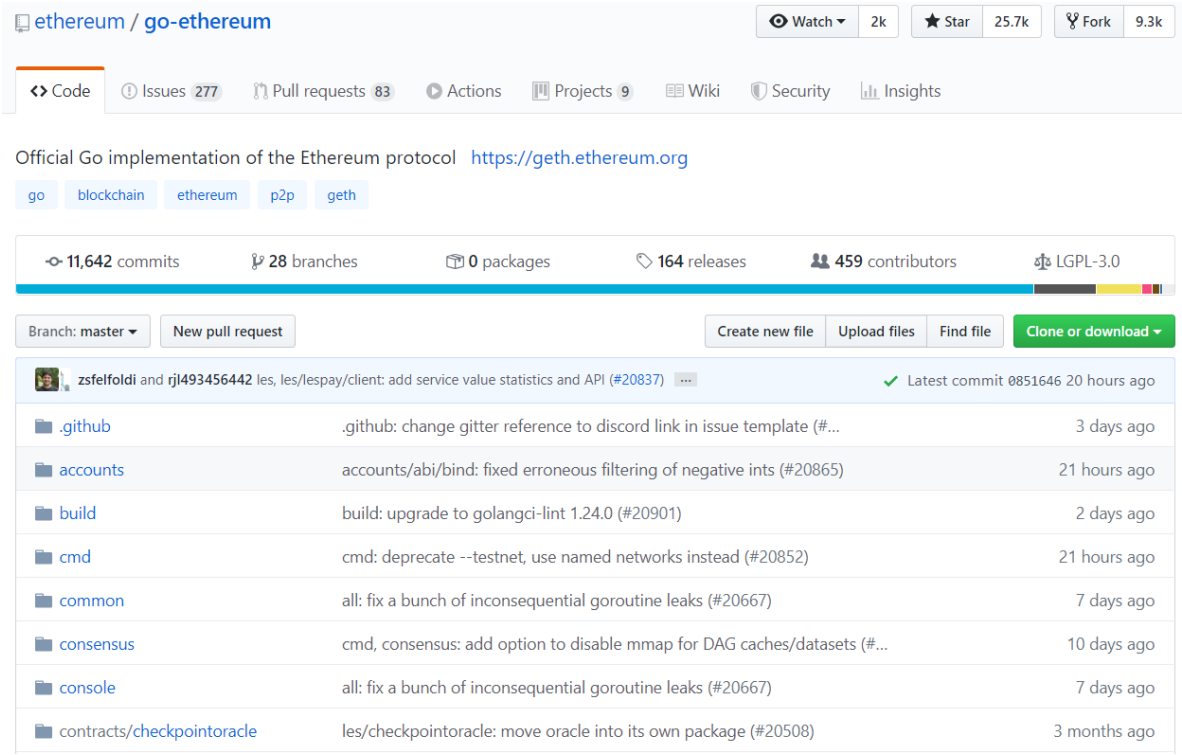


2.2 Open-source projects on GitHub

2.2.1 go-ethereum

As we know, Ethereum(以太坊) is one of the most famous open-source public blockchain platform with smart contract capabilities that provides a decentralized Ethereum Virtual Machine to handle peer-to-peer contracts through its proprietary cryptocurrency Ether(We will focus on Ethereum--Application of block chain and smart contract on the Part 3 of our report)

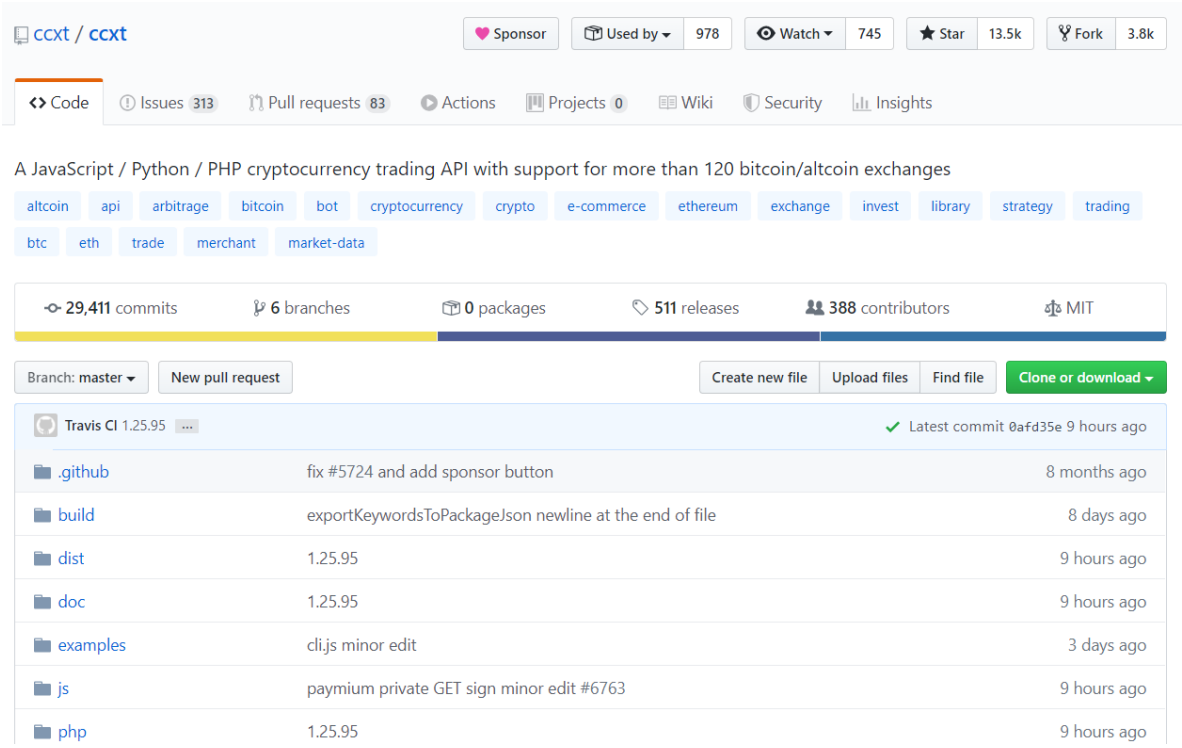
And go-ethereum is a official **Golang implementation of the Ethereum protocol**. You can find the open-source project on https://github.com/ethereum/go-ethereum. The project has more than 450 contributors and received more then 25.7K ☆ on GitHub



2.2.2 CCTX

CCTX's full name is CryptoCurrency eXchange Trading Library, which is a JavaScript / Python / PHP library for cryptocurrency trading and e-commerce with support for many bitcoin /ether / altcoin exchange markets and merchant APIs. The **CCXT** library is used to connect and trade with cryptocurrency exchanges and payment processing services worldwide. It provides quick access to market data for storage, analysis, visualization, indicator development, algorithmic trading, strategy backtesting, bot programming, and related software engineering.It is intended to be used by **coders, developers, technically-skilled traders, data-scientists and financial analysts** for building trading algorithms, which can algo give support to the backend development using Develop Flame like Python Flask/ Django and PHP.It can support for many cryptocurrency exchanges and fully implemented public an privare APIs, which can also provided optional normalized data for cross-exchange analytics and arbitrage.

This open-source project has 388 developers now and received more than 13.5K ☆ on the GitHub. It is also a popular open-source project. What's more, we find another API library for Javascript in the Ethereum development called **Web3.js**



2.2.3 Solidity, the Contract-Oriented Programming Language

As mentioned above, the development of blaockchain and smart contract application system is mostly based on the traditional WEB development using Javascript, Golang, Python and their develpoment flameworks with new APIs also implemented by those langauge. But this open-source project creating a totaly new language named solidity to develop the smart contracts. Solidity is a statically-typed curly-braces programming language designed for developing smart contracts that run on the Ethereum Virtual Machine. Smart contracts are programs that are executed inside a peer-to-peer network where nobody has special authority over the execution, and thus they allow to implement tokens of value, ownership, voting and other kinds of logics.

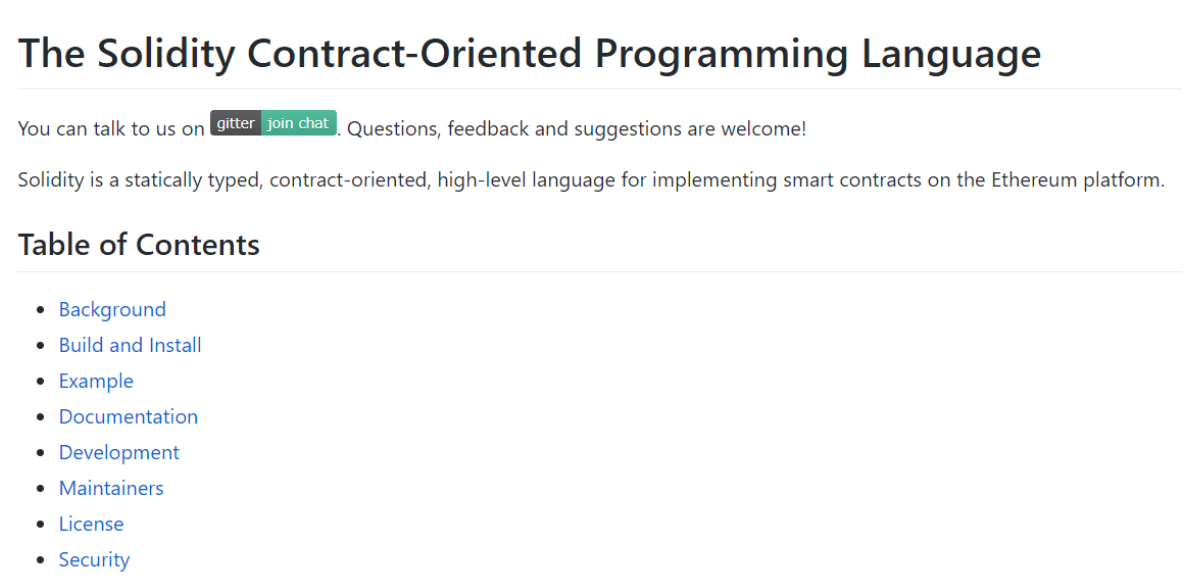
When deploying contracts, you should use the latest released version of Solidity. This is because breaking changes as well as new features and bug fixes are introduced regularly. We currently use a 0.x version number to indicate this fast pace of change.

This project gets more than 7.8k ☆ on GitHub and 342 conttributors contribute their code to this project.

```
pragma solidity ^0.6.0;

contract HelloWorld {
  function helloWorld() external pure returns (string memory) {
    return "Hello, World!";
  }
}

//a "Hello World" Program using the solidity language.
```



2.3 Startups in Block Chain business

As the open-source community has a good atmosphere of developing, there are also many startups in the field of block chain field. They get good success in block chain platform. The block chain and smart contract have several develpoing steps like bit-coin and Ethereum, and now the cutting-edge applications of block chain have been in a new phase, based on the traditional technology of block chain and smart contract. According to our research, we find many innovative business constructed by block chain and related technologies.

We found that block chain can be used in many fields like security computing, financial industry, Internet Media industry and online-shopping. These are the business opportunities discovered by the flowing startups.

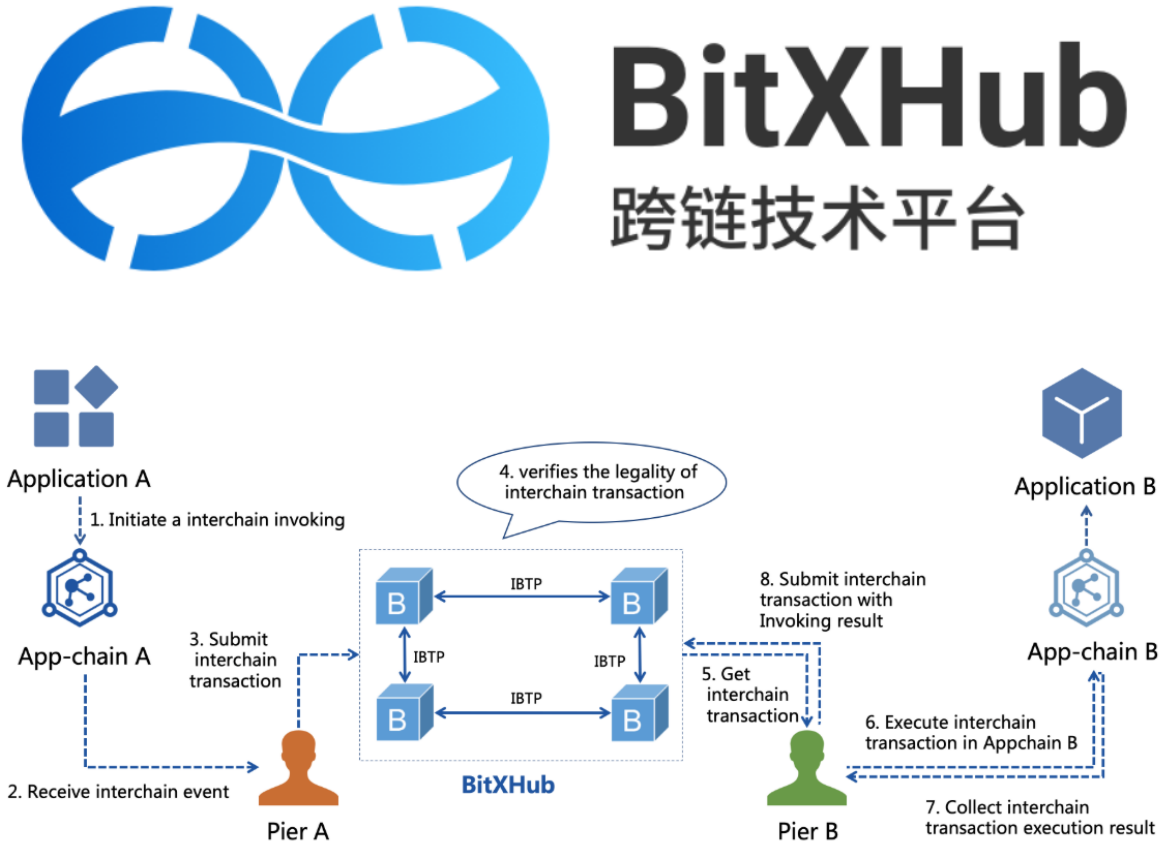
2.3.1 HyperChain(趣链科技)

HyperChain(趣联科技) was was founded in 2016, focusing on blockchain technology products and application solutions. The main products are: the domestic independent controllable block chain underlying platform, data sharing and security computing platform **BitXMesh**, block chain open service platform **FiLoop**, supply chain finance platform **FiloLink**, storage service platform **FiloInk**, smart contract security research and development platform **MeshSec**.

At present, the company has applied for more than 208 patents and obtained 57 software Copyrights. Published block chain professional work "advance and practice of block chain technology"; Participated in the formulation of more than 20 international blockchain standards, 2 national standards, and more than 20 group standards, totaling more than 50 items, of which 7 items have been published and applied to the credible blockchain promotion plan of the information communication institute of the ministry of industry and information technology; Participated in the preparation of the white paper on blockchain (2018) of China academy of information and communications and the credible blockchain, and the blue book on blockchain of the people's bank of China (2018).

What's more, it's worth mentioning that the founders of this startup company is a 'ZJU group', many of the founders and core members are graduated from Zhejiang University.

The technical team of HyperChain also share their research and develoment on the open-source community, such as BitXHub, which is is committed to building a scalable, robust, and pluggable inter-blockchain reference implementation, that can provide reliable technical support for the formation of a blockchain internet and intercommunication of value islands.

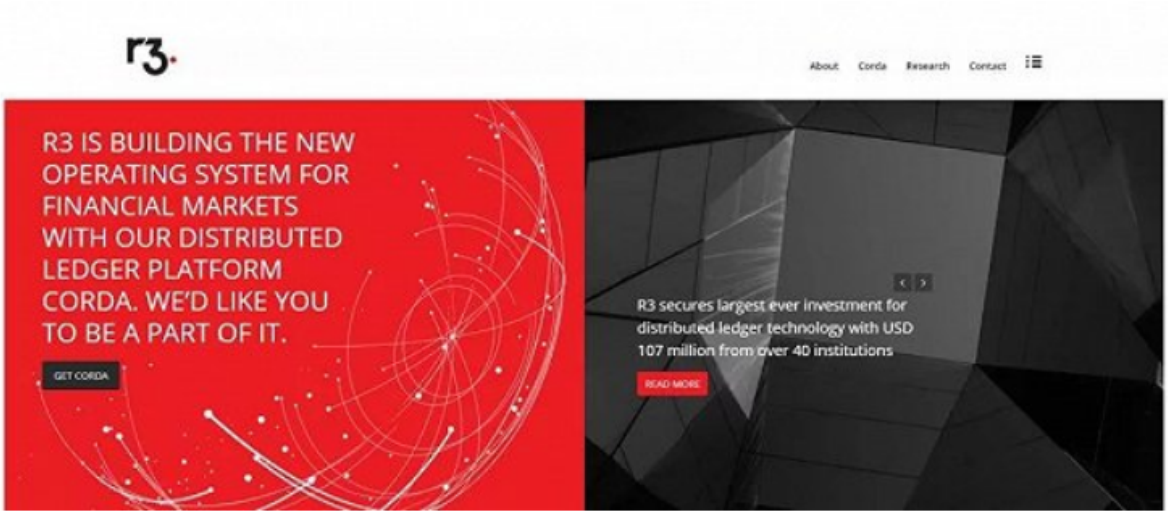


Architecture of BitXHub

2.3.2 R3

R3 is a company focusing on application of block chain in financial industry. Block chain can provide higher accuracy and information sharing for the financial services ecosystem because of its distributed ledger and features of tamper-proof. In financial area, R3 (R3CEV LLC) is more of a distributed database technology

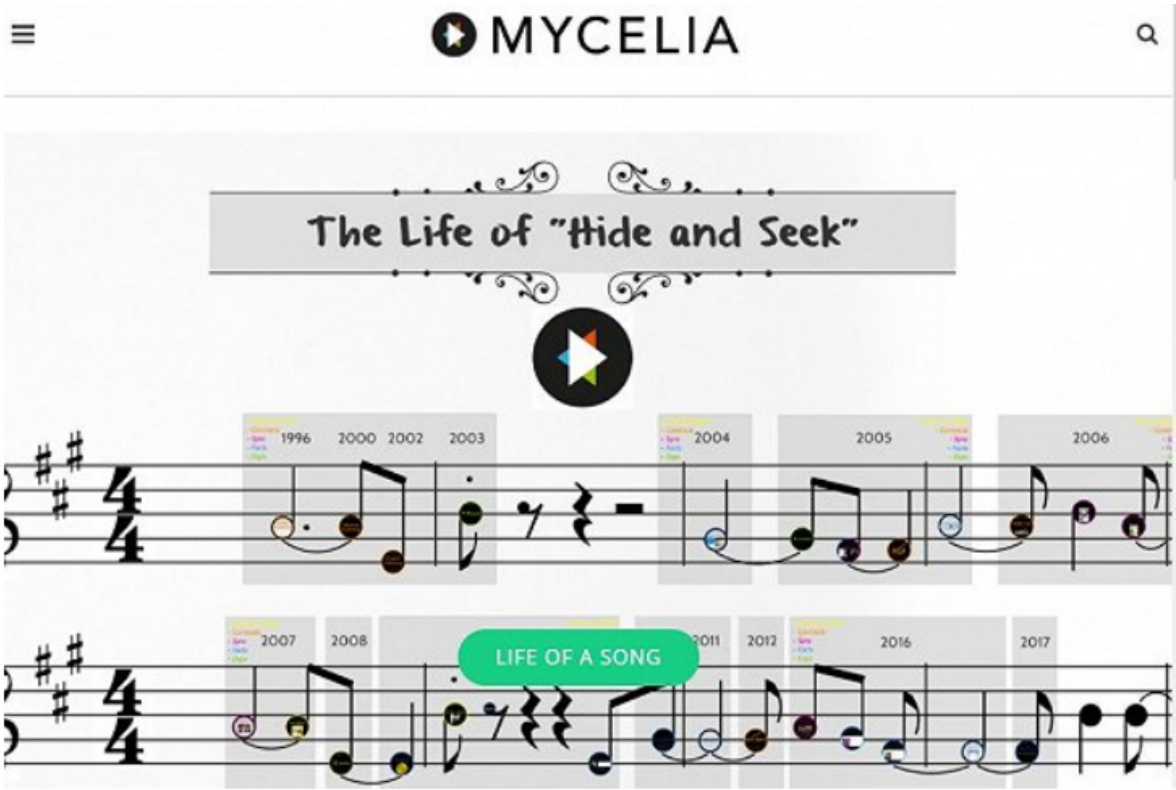
start-ups, founded in 2014, they, now with more than 80 member Banks, regulators and technology partners to jointly develop Corda, open source platform for the distributed books, through decentralization technology, to complete the bank reconciliation between straight league.



2.3.3 Mycelia

Mycelia is a company provide a platform based on block chain for technology companies, record labels, collective management organizations, streaming platforms and, most importantly, originators at the heart of the industry.

Founder of Mycelia Imogen Heap thought, through the block change cultural industry chain, based on the intelligent content under the contract, can be spread and more equitable sharing, to some extent help to protection of rights and interests of the creator, and in this process, the creative work of buying income can be released automatically according to the predetermined license agreement, Mycelia also is trying to it.



2.3.4 Farma Trust

FarmaTrust helps save lives by using immutable records to monitor drugs from point of origin to point of consumption, the system tracks the path of drug flow, eliminates inefficiencies in the pharmaceutical industry, and fights counterfeit drugs. Currently, FarmaTrust is used by relevant practitioners worldwide, and according to reported data, FarmaTrust has saved nearly one million lives every year.

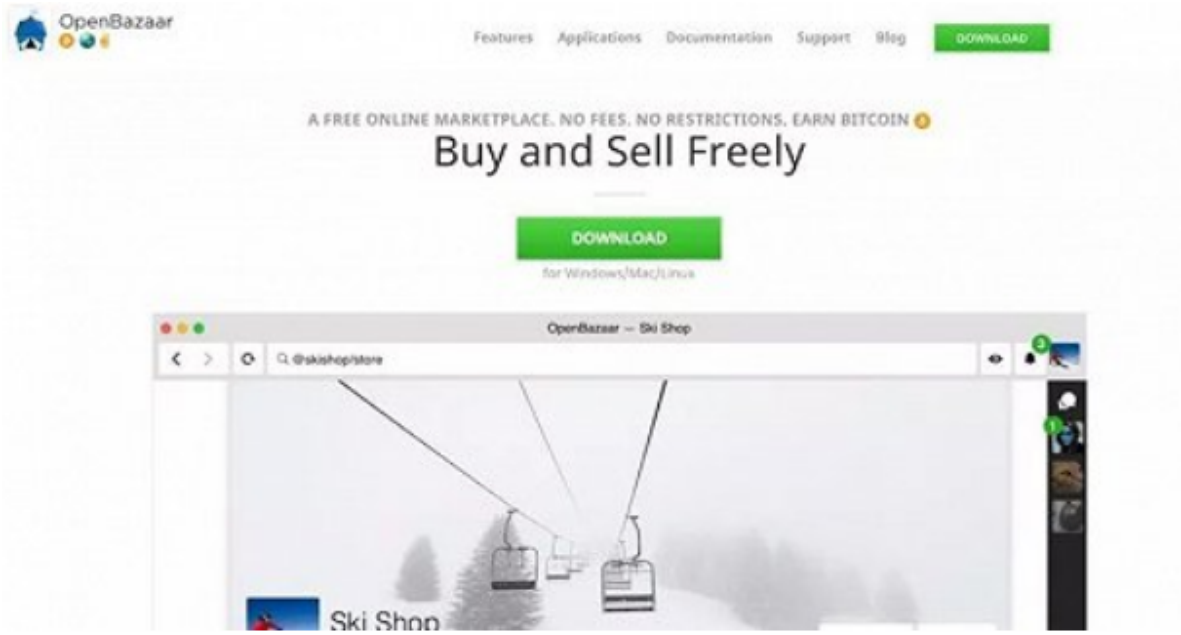
At the same time, in the healthcare sector, it is becoming increasingly important to share medical data across platforms through blockchain technology to improve the possibility of effective treatment and the overall ability of healthcare systems to provide effective care. To that end, Gem, a startup, launched healthnet, a multinational blockchain network that spans the entire healthcare sector, creating a secure, common data-sharing infrastructure using ethereum blockchain technology. Tierion is another blockchain startup that builds a platform for storing and validating medical data. Gem and Tierion are currently working with philips healthcare on blockchain LABS. The value of blockchain technology in the medical field is gradually emerging.

2.3.5 OpenBazaar: a future TaoBao

Consumers' trust in the retail system is mainly related to their trust in the market where they are shopping (for example, some media believe that trust is the key factor for amazon to acquire users). Blockchain, on the other hand, can spread that trust, attaching it to sellers on various markets and platforms rather than to the site itself.

Therefore, the startup OpenBazaar is developing a decentralized blockchain public network to connect buyers and sellers without middlemen or fees. According to reports, OpenBazaar is an open source peer-to-peer network that offers free and unlimited sales to merchants and is a decentralized global marketplace for free buying and selling. Customers can use any of 50

cryptocurrencies to buy goods, sell and pay in bitcoin, and all the data is distributed across the global network. There are even users who believe that Openbazaar, whose local currency is bitcoin, has the absolute potential to be the taobao of the future.



2.4 Conclusion

All in all, in this part of report, we could learn that the block chain and smart contract have a pretty good ecology and development depends on the open-source community and emerging startups. The pretty good ecology is a significant premise condition for the further development of a technology especially in computer science field.

It is a benign mechanism that the open-source community and startups promote each other, some open-source technology has become Business products by the operation of startups, and the developers in those startups in the startups make their technology of block chain and smart contract open-source, which leads to a virtuous cycle.

Chapter 3： The challenge and Future of Block Chain and Smart Contract

Although block chain and smart contract technology have made amazing progress, there are still many factors restricting the long-term development of such technology. In fact, the nature of block chain is called a distributed finite state machine with an untamable state file. Ethereum's Yellow Book has a strict definition of block chain, which is defined in a mathematical language. In the definition, block chain is an ideal state of complete de-centralization, trust, security, fairness, privacy, efficiency, accountability, and self-organizing, self-governing society.

Ethereum's vision of block chain is a great dream, but why it is so hard to achieve? We think that one of the main reasons is that, the main purpose of traditional computer technology is to improve the production efficiency of computers, while the main goal of block chain is to improve the **production**

relationship of computers. The current limitations of block chain technology are mainly in the distributed system to make all nodes unified, and the constraints can be summed up as the following ten points.

1. Performance limitations
2. Limitation of scalability
3. Usability limitations
4. Limitation of compatibility
5. Storage limitations
6. Rigorous mathematical proof
7. Formal verification
8. Synchronization restrictions
9. Governance constraints
10. Limitations on software upgrades

And the technologies should be improved in the future development of block chain are:

1. Performance and scalability
2. Security of blockchain
3. Privacy protection
4. Authenticity of data
5. Password security
6. Identity authentication and authority management
7. Governance and supervision
8. Prevent centralization

A popular theory about block chain and smart contract is that block chain 1.0 is represented by bitcoin, a programmable digital currency that actually uses a non-Turing complete scripting engine to control the execution of UTXO transactions. What's more, block chain 2.0 is represented by Ethereum, which actually represents programmable finance. Unlike bitcoin, it is promoted from the UTXO state of pure asset transaction to the support of programmable intelligent contract of world state.

Along this line of thought, block chain 3.0 can be a programmable organization and a programmable society in the future with the help of smart contracts. This prediction now looks a little far from out real life. So the 3.0 block chain everyone talk about is, in fact, in order to solve the etheric fang couldn't solve some problems, especially in terms of performance problems, many brand chain 3.0 the block chain platform, most are still in a development stage, but gave us a very high TPS, vision is very safe and reliable.

We have enough reason to believe that the block chain will make great breakthrough in the future, with the development of smart contract. And the following fields will be the focus point, including block chain operating system, block chain middleware, block chain network direction, enterprise-level block chain, block chain storage, anti-quantum algorithm, scene applicability innovation, and many other new directions.

Chapter 4: References

[1] Don D.H. Shin. Blockchain: The emerging technology of digital trust[J]. Telematics and Informatics,2019,45.

[2] Decker C, Wattenhofer R. Information propagation in the bitcoin network [C]//The 13th IEEE Conference on Peer-to-Peer Computing, Trento: IEEE 2013: 1-10.

[3] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable block chain protocol [C] // Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, 2016: 45-59.

[4] Sompolinsky Y, Lewenberg Y, Zohar A. Inclusive block chain protocols [C]//International Conference on Financial Cryptography and Data Security, Heidelberg: Springer, 2015, 8975: 528-547.

[5] Duong T, Fan L, Zhou H S. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely [EB/OL]. (2017-04-14) [2018-09-30]

[6]https://github.com/ccxt/ccxt

[7]https://github.com/ethereum/solidity

[8] https://github.com/ethereum/go-ethereum