Celes Chain WhitePaper

TechnicalWhitePaper

Version:Beta 0.68

2018 Jun

C链
Celes Chain

Executive Summary

The white paper describes the top hierarchy design for Celes Chain (also refers to “CC Platform” or C Chain or CC below). CC is an innovative blockchain platform to run financial services / applications and provides access for regulators and compliance departments. It reduces the cost of regulation and increases efficiency. Financial Institutions who uses Celes Chain can reduce cost of implementations, increases revenues and enhance return on capital. Users of the financial applications can have better services with higher quality. The white paper provides the blueprints, logics, system design and other non-technical information related to the designing the Celes Chain. This is a beta draft version. Readers should be aware that the team (Celes Chain team) might revise this whitepaper in a continuous basis.

Celes Chain uses decentralized consensus and blockchain techknowledge to support financial applications, including but not limited to: information providers, service, cross-border applications, investment and banking IT supports. CC allows multi-participants including financial institutions, regulations / compliances departments and end users. CC platform can support a large scale of the applications with safe applications.

We use a consensus, so called “Time Division Multiple Proofs Consensus Protocols” , TDMPC Protocols [1]. TDMPC can achieve a good balance between “decentralization” and “efficiency” . This consensus could make our CC platform: (1) true decentralization through the miners competitions; (2) miners have enough motivations to invest enough and stable hardware to support a large scale of applications.

We are going to develop and use a unique script language, Celes Chain Services Languages (CCSL). It would be a powerful and intuitive turing complete script language for financial applications. The participants from CC platform can use this power CCSL to implement their financial and business logics to write smart contracts [2]. Participants can abstract the common logics to develop script languages templates for other participants to import directly. Also, the regulators can monitor and regulate the applications, data and participants behaviors according to the laws. CC will compile part of the protocols, applications, codes and data into legal documents for further compliance. Moreover these data and documents can be encrypted and hashed, and then write into the blockchain to prevent to be stolen and alternated.

At the beginning of the whitepaper, we will briefly describe the overview of finan-cial industry as well as the current blockchain technology. We will continue dis-cuss how to think and solve the issues: (1) the balance between “efficiency” and “decentralization” , (2) how to have a large scale of applications running on the platform, (3) how to safeguard the user’ s information and effective regulations. These discussions eventually lead us to finish the design of Celes Chain, building the wallstreet on the blockchain and providing services for financial institutions. We will also discuss the functions for different levels in CC, tokenized applications and the ecosystem.

Contents

01 Introduction

1.1 Current Financial System

The wallstreet has been leading the financial innovations since year 2000. However, such innovations usually come with high leverages and complexity. A global financial crisis breaking up in 2008, eventually destroys the confidences to the financial institutions [3]. In order to save the financial system, boost up the confidence and recover the economy, the governments and central banks implement aggressive monetary policies [4], inject liquidity and tighten the regulations [5], which stop the economy from slowing down but also bring back the concerns on inflations and currency depreciations.

For a tighten regulations, Europe implements the MIFID2 [6] and USA implements the Dodd Franks / Volcker rules [7] to regulate the financial institutions, especially for OTC transactions. This comes with a price of a very high regulation cost and lacking innovations. Small financial institutions are more difficult to compete with the big ones, which increase the degrees of being “centralization” , more and more financial institutions become “too big too fail” [8].

1.1.1 European MIFID2 Regulations

The EU has been working on the MIFID2, short for Markets in Financial Instruments Directive II, for more than 8 years and with more than 1 millions paragraphs of contents. It will be implemented after January 2018. The major goal of these regulations is to prevent the next potential financial crisis with three measurements: (1) transparency of the trading, (2) demands exchanges and venues to provide data and continue clearing the OTC trades. (3) enhancing the regulations. [27]

For European financial institutions, the implementations might decrease the profits I with substantial investments. According to Boston Consulting estimates [28], $ 2.1 billion was spent in 2017 alone, not counting the incremental investment and expenses that were incurred in future specific practices, and the actual cost of doing so is still hard to be estimated. Because of the heavy investment in MIFID2, financial institutions will spend $ 3 billion less on research for financial innovations. Also, there would be a significant impact on about 20% investment banking business in Europe.

In addition, according to a report from Sina finance [29], "MIFID II requires huge amounts of data to be recorded, posing a significant technical challenge to the banking industry." As of December 2017, 17 EU countries still do not have MIFID2 related laws implemented. It is believed that the technology is one of the major issues of the implementation.

1.1.2 US Dodd–Frank and Volcker Rules

The Obama administration launched the Dodd–Frank Act against the financial crisis after 2008, with the main purpose for protecting retail investors of financial products. This act plays an important role in restoring the confidence of the financial industry. However, financial institutions have paid huge compliance costs for the bill.

An estimate was made by the American Action Forum [30] that the financial industry spent $ 36 billion and up to 7.3 million work–hours just to prepare a written document for the act. According to reports, the bill has released total more than 22,000 pages [31]. In addition to the financial industry's huge cost, the federal government hired more than 2,600 full–time, professional federal employees to manage the bill over the first five years of the law and cost the taxpayer $ 3 billion.

In addition, the US Volcker Rules, is a regulatory act that provides guidelines for the self–regulatory of the banking sector. Reuters reported in 2014 that the bank's compliance costs hit $ 4.3 billion every year.

1.2 Existing Blockchain Technology

With the rise of cryptography, many pioneers have begun to explore the cryptocurrency and attempted to make some improvements to the current financial system: aggressive monetary policy and the cost of regulations.

1.2.1 Bitcoin

Bitcoin [9] is the first decentralized cryptocurrency in the world that is widely used in practice. The Proof of Work (PoW) proves that such consensus can effectively solve the "the Byzantine Generals Problem" for its almost 10 years of practice [10]. The basic principle is that all nodes store and verify all the historical accounts, and then use PoW to reach the one and the only one consensus of the entire network on the next ledger.

As the proof of work requires the commitment of computer power investment in advance, it can effectively avoid the hacker attacks. It does not need to have a third party trust and intermediary facility. It is a point-to-point electronic cash system. As miners are working to maintain the safety of the Bitcoin network, all nodes in the Bitcoin network reached a consensus that a certain amount of bitcoin should be issued to the miners as a fixed reward plus transaction fees within the current block. The fixed reward is halved every four years, so the total number of bitcoins converges to 21 million. Because Bitcoin's coin forging is generated 100% by mining, Bitcoin's forging is well-established and well-regulated in advance. And the amount of bitcoin in the entire network is a constant, which solves the inflation problem caused by aggressive monetary policy. However, bitcoin also has problems such as slow clearing [11], waste of power [12], and the scale of applications [13].

1.2.2 Ethereum

Ethereum is the second largest blockchain network in the world [14]. Ethereum is invented mainly to solve two problems from Bitcoin. Ethereum added "Turing complete" scripting language to support "smart contracts" [15]. These smart contracts can be self-running on the Ethereum network and stored permanently without being tampered with. Through these "smart contracts", users can develop DApps (Decentralized Apps) [15] on Ethereum. Ethereum also uses PoW consensus "elect" nodes to run these smart contracts. Like Bitcoin, Ethereum is decentralized.

However, because Ethereum is a "public chain", smart contracts between counterparties will be seen by other parties that do not want to do anything, which makes it impossible for Ethereum to run some applications that need privacy protection and user information security. So in order to run this type of application, but also need to make some corresponding changes. Barclays, UBS and Credit Suisse have all tried to use their "modified" Ethereum network to advance their internal compliance with MIFID2 [16]. According to ibtimes reports, the modified "Ethereum Network" may sacrifice the "decentralized" use of a private chain or affiliate chain to solve user information security issues [17].

Because of the competition of the PoW, the nodes in Ethereum network do not have enough incentives to invest in hardware resources to run large-scale applications. The famous "cyrpto kitties" at the end of 2017 in the Ethereum network, causes traffic jam in the Ethereum system and other ordinary transactions varying degrees of latency.

1.2.3 Other Technology

Other pioneers have also tried to solve Bitcoin or Ethereum problems by modifying the existing consensus system or create a new one. Daniel Larimer founded EOS.io project which uses the Delegated Proof of Stake (DPoS) [18] to reach a consensus by using an electoral representation instead of mining. The obvious benefit of this approach is that the electorate elected by the Electoral College is relatively stable and cooperative that has more motivations than Ethereum to invest in hardware resources. However, there are also some arguments that DPoS does not prevent an monopoly that manipulates the entire EOS network by controlling the entire representative team with multiple IDs and EOS becomes a truly centralized network [19].

There are other teams, such as R3 or Digital Asset Holdings, have tried to use private chains or other compromised solutions. Such solutions might make smart contracts effectively executable as well as give compliance and regulations an easier access to the financial industry, but it compromises the degrees of "centralizations". In MAS's Ubin project phase 2 report [ref], the degrees of centralization increases when smaller financial institutions have less incentives to join the chain. From this we can see that if we need to resolve the contradiction between "decentralization" and "efficiency" and "privacy," we still need to think from the consensus at the bottom level.

1.3 Celes Chain Is The Solution

Celes Chain, CC is a decentralized blockchain platform that provides the bottom IT services for a variety of financial applications. We want to create the "Wall Street" on a blockchain that serves a wide range of financial institutions and users. We use innovative consensus algorithms that can be truly decentralized with efficiency. In addition, we will also design a special scripting language to support smart contracts and various applications. CC is designed to provide a full range of support for efficient regulatory and compliance with local regulators. We will achieve this by implementing a dedicated regulatory compliance layer. The regulatory compliance compilation layer is responsible for compiling smart contracts into legal documents.

By reducing operational costs and increasing regulatory efficiency, Celes Chain can attract the regulators, financial institutions and end-users to use this platform.

1.3.1 Celes Chain's Top Hierarchy Design

In the system design, we adopt TCP / IP–like protocol hierarchy (refer to Figure 1) and implement it with application layer, legal / compliance layer, data layer as well as the consensus layer. It ensures that the levels can communicate with each other.

Participants

Figure 1 Celes Chain System Design

1.3.2 Regulators Uses Celes Chain: Less Cost and be More Effective to Prevent the next Potential Financial Crises

In order to prevent the next financial crisis, the regulators, including the central banks, securities agencies or other financial regulators, are using a remedial measure: first of all, they try to repair the existing compliance systems and then upgrade the IT technology. Finally they try to improve the whole system. Although this approach is easy to get started, there are also huge drawbacks:

(1) Huge amount of data to be processed: This includes the amount and timing which the industry needs to submit through their old systems. Also regulators need to have a new system ready to process such big amount of the data. It would be a huge challenge to the bank's IT system.

(2) Legal Documents and Regulatory Costs: Every single bill has a vast of documents with high enforcement costs.

(3) Social costs can be as high as hundreds of billions of dollars and tens of millions of working hours. In addition to the social costs, it can also cost the government billions of dollars. And such project usually is a progressive development, and it is difficult to predict the total cost.

(4) It could take years for the implementations even if the financial institutions are willing to cooperate.

First of all, our Celes Chain is a public-chain blockchain system that uses innovative consensus. The data generated by those financial applications built on our system, are not able to be falsified. They are also transparent and visible to regulatory compliance and analysis. It easily solves the first problem above.

Second, all the laws, regulations, and smart contracts are stored in Celes Chain in the form of codes and executed automatically by the Celes Virtual Machine (CVM), effectively solving the second problem above.

Like the other financial institutions, government regulators conduct their financial activities by participating in regulation activities on Celes Chain and pay a certain amount of token to miners. Since the miner operations are fully decentralized and competitive, the regulatory costs will be significantly lower than the regulatory costs currently required.

In theory, any regulation implemented on Celes Chain is considered to be "real-time". Regulators can also do a variety of "stress tests" if needed. By using a common platform, financial institutions will be much faster than traditional way when they try to adopt to new regulations.

Although regulation at Celes Chain can save hundreds of billions of dollars in costs and is highly efficient, regulators do not need to force financial institutions to use the platform through additional laws and regulations. The only thing the regulators need is to be compatible with this Celes Chain, and financial institutions will voluntarily choose to use Celes Chain because of cost and efficiency considerations. In addition, because Celes Chain is a public chain, this reduces the doubts of financial institutions when considering to participate the chain.

1.3.3 Financial Institutions Uses Celes Chain: Cost Saving and Return Increasing

There are many reasons why financial institutions should choose Celes Chain, but only this one is the most important: to increase shareholder return. Financial institutions can increase shareholder return in the following ways.

(1) Reduce the costs of regulation, compliance and arbitration: The theoretical costs for financial institutions to respond to various types of regulation at Celes

Chain can be almost zero. In the most extreme circumstances, some financial institutions might have their profit before tax increased by 30% [32]. Moreover, as regulatory compliance becomes more transparent and contracts are written and stored on Celes Chain, this will significantly reduce the costs of arbitration due to disagreement.

(2) Reduce the operation cost from the back office : the use of smart contracts can greatly reduce operational risk. Because smart contracts are automatically executed by virtual machines and settled.

(3) Reduce possible losses: The use of blockchain / public chain can be more effective in managing counterparty risk.

(4) Generates more profits: financial institutions can access a larger market more easily and quickly to develop valuable products.

1.3.4 Final Users of Celes Chain Could Have a Safe and Effective Service

Users use financial services through Celes Chain for better pricing and security. As financial institutions can produce financial products with lower costs. At the same time, the users can enjoy lower prices and higher quality of service. End-users can easily identify whether the purchased product is in compliance with regulation; with a proper risk disclosure and safe.

1.3.5 Choice of Public Chain or Private Chain

Currently, most of the financial institutions want to use the private chain as their choices of blockchain. But the private chain is not the most optimal solution, because the participants of private chains usually do not share the same interests with the private chain leader. Also, the smaller ones do not want to invest resources to join other's chain.

Financial institutions should choose a suitable chain, for example, Celes Chain, because the chain has no leader or natural monoplayer. That's why it is able to attract the financial institutions to join.

02 Celes Chain Overview

This chapter has two parts: the description of user groups and the structure de–scription of several layers. As shown in FIG. 2, the architecture of the system for each user group is the same, but each user group has different access level which will be illustrated further in the next chapters.

Celes Chain System Diagram

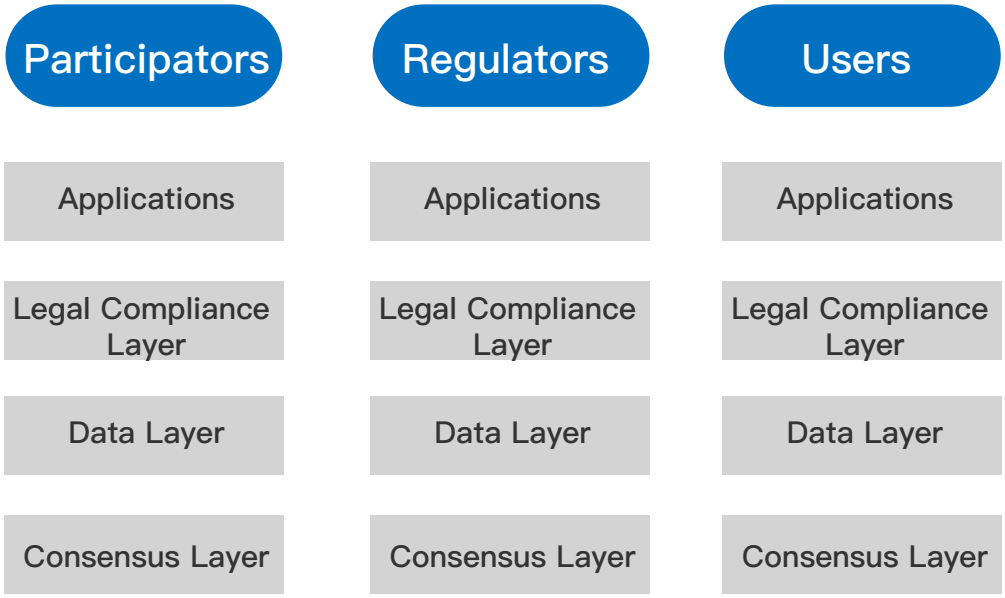

Figure. 2 Celes Chain user groups and layers

2.1 User Groups

Celes Chain's user base includes: participators, regulators, users.

Participator mainly refers to the institutional participants. They implement the business logic on the CC. They also develop applications and provide services for users. Similar to common financial institutions, participants have the ownership of their business logic / applications and are responsible for the data security.

Regulators and Administrators, which include the the regulatory compliance agencies and qualified CC network regulators, are primarily responsible for reviewing the services on CC if they are in compliance with the regulations. The regulators have greater power than the other participants. In other words, the regulators are "super administrators" in the CC that regulate CCs and their applications in all dimensions and directions.

Users are (1) basic units or individuals that use the application services on the CC, and (2) network nodes that maintain the underlying consensus and CC operation.

2.2 The Role Of Regulators and CC’s Compliance Efforts

We have specifically come up with this section to describe in detail how the CC is coordinated with regulations and laws, to provide all participants with the underlying services. First of , we set this special user group of regulators to give this user group maximum access to all levels, all data, and user information throughout the CC, according to the local laws. This user group is designed to those qualified financial participants and CC network administrators.

Regulators will watch the applications available on CC network and ensure that the products and services and suitable for qualified users. For example ,some products which are for professional investors should not be sold to normal investors.

In addition, when designing Smart Contract CC Scripting Language, Celes Chain will adopt a scripting language that can work with different legal systems to ensure the participants are free to choose the methods are required to comply with legal compliance. Our goal is to have the code as the same as legal documents. However, legal and compliance varies considerably from country to country, and there are time-sensitive issues. Therefore, CC also has a layer of legal and compliance compiler responsible for compiling the code into realistic and legally-readable texts by using templates or deep learning methods.

Because CC uses "decentralized" blockchain to record key data and witness, regulators can get any data and records, so the current financial applications cost of various compliance filing, such as MIFID2, etc., on the CC Do the application, then there will be greater savings. At the same time because of the existence of the blockchain, CC service does not exist in theory to conceal or distort the transaction data. The Celes chain is working from both the "consumer", "code"

and "text" levels to monitor and strive to be compliant with development services across this blockchain.

2.3 Layers Setting

Celes Chain has four layers: the application layer, legal compliance compilation layer, data layer and the consensus layer:

The application layer mainly solves five problems: (1) the communication with users, (2) a platform for participants and regulators to implement business logic, including CC scripting language and CC virtual machine. (3) The applications are supervised by regulators and listed on the CC application "store" (4) In order to improve the efficiency, participants and users of the same functional category can share a template to save resources and costs. (5) The CC scripting language is designed to be used and compatible with the legal systems. And the codes will be written in CC scripting language. The legal templates will be generated by a specialized legal compliance layer and recorded in the data layer .

Legal compliance layer is a module that the CC will specifically design to meet regulatory requirements. All applications, codes and templates produced in the CC scripting language must be in legally compliance with a proper signature. The participants can choose which legal system to use when coding or compile the codes into legal documents.

The data layer is where the CC stores data and witness of evidences. Data are generally divided into three categories: (1) data to be witnessed, settlements or signatures, etc. (2) business logics, user informations, contracts, smart contracts, and (3) other data.

The participants according to the cost and privacy levels to choose below methods: (1) Encrypted data written into the public chain (2) Witness written into the public chain (3) Data written into the application's own database (4) Data written to the public database.

The consensus layer uses the time–division multiple proofs consensus protocol. The TDMPC uses PoW (Proof of Work) to get the "wood" and asynchronously use the "wood" for PoB (Proof of Burn) [ref] to generate tokens and generate blocks. This enables the CC to achieve a better balance between the decentralization and efficiency. It also gives the the miners enough incentives to invest hardware resources. This makes sure that the efficiency and stability of CC chain is as good as other private chain [1].

03 Application Layer

Logically, the application layer is divided into UI Sub Layer, Business Logic Sub Layer, and CC Virtual Machine three parts.

The UI Sub Layer mainly focus on the interaction between the user and CC applications, including but not limited to providing interfaces, forms, various types of input, output / display, authentication portal, cross-platform , API Service and more.

The CC Business Logic Sub Layer primarily provides the tools for users to write the business logic: this includes services such as code, applications, smart contracts, and smart clearing / settlements. CC business logic is based on a scripting language designed for CC platform. In addition to providing Turing Complete logic [33], this script language also is compatible with legal and compliance to develop business logic and documents into the next data layer. It would be ready for regulator inspection for the approval to be listed in CC store for other users to use..

CC Virtual Machine is a definition of the computer resources from the public chain nodes. Virtual machines support and run CC business logic by consuming their node resources, including code, applications, settlements, data processing, and more. The virtual machine will also get a certain amount of rewards. The rewards and the consensus of the public chain will be further elaborated in the sections below.

3.1 UI Sub Layer

The user interface sub-layer connects the users and next sub layer of business logics. The CC platform also provides APIs for professional users to execute programmatic strategies on different platforms, download various types of data, and even breed the API Economics for wholesale and retail data. Moreover, it is also possible to enhance the user experience through interaction with VR / AR. The API Economy and AR / VR are not the focus of this white paper discussion and will not be further discussed.

3.2 CC Business Logic Sub Layer

This level is for the participators to write the business logic. In our Celes chain, the business logic is defined as services such as code, applications, smart contracts, and smart settlements.

CC will specifically develop a set of CC script language. At the same time, the CC evaluates the computer resources consumed to run the logic. The definition of computer resources and the ecosystem of CC will be described in the later chapters. The business logic developed in the codes will be run by the virtual machine in the decentralized network. Once it is created, business logic can not be changed without authorization.

SEC believes that the computer codes could be a legally binding contract [20]. When we develop the CC scripting language, we also take into account how we can fit the code and the current law together. We will try to develop appropriate script languages for different legal systems (civil law or European and American legal systems). And we might incorporate more details for for different countries and different regulatory agencies. We strive to develop a new generation of scripting languages that can deliver both coding and legal binding.

The business logics and documents developed will be stored in the next level: database layer. The regulators will exam and grant the permission to access to the CC application stores.
CC's business logic and app store will be similar at Apple's App Store, which the app developers have the ownership of the applications. Obviously, whether the application can be listed or delisted on the stores, apart from the permission from the regulators, the miners will also judge based on the "economic" principle to choose whether to implement and run the application. In other words, in the CC, any application should produce value, and the value is greater than its running costs.

3.2.1 CC Smart Script Languages, CSSL

CC smart script language, CSSL, is used to develop the business logic of CC, including services such as code, applications, smart contracts, and settlements. CSSL will have: Turing complete, assessment of consumption, automatic execution, compatible with legal compliance, easy-to-use and privacy protection features.

◆ Turing Complete

First of all, CSSL will choose a Turing complete scripting language similar to Ethereum, including the logic of loops. However, in order to maintain the network stability, CC will limit the maximum number of the loop cycles. According to the concept of a universal Turing machine, Turing complete is what modern programming languages can have and can achieve the highest computational power of the von Neumann architecture. In general, most computer languages are Turing-complete, except for a subset of scripting languages, such as the scripting language native to Bitcoin. Using Turing's complete scripting language, CSSL can be logically made compatible with other programming languages and in theory can be implemented in any other language with achievable logic.

◆ Consumption Assessment and Analysis

Since CC is a public chain system, nodes will choose the applications which have better economics: a higher ratio of revenue to occupied computing resources. So before any code is executed, CC will evaluate the CPU, memory, storage resources and bandwidth it may use. One of the criteria for the evaluation can be, but is not limited to: (1) Estimating the number of the operators, i.e. the computational complexity (2), and the number of variables (3) the length of the codes.

CSSL allows the external input to interact with the contract. This external input must be maintained by a qualified participant and the participant must make a estimation of the possible value and the range of the inputs.

The miners need to price the basic unit of consumption.

It is important for them to have enough information to estimate the average price of the each operator in the whole network, by (i) the calculation of the entire network and (ii) the distribution of the “woods” . This allows the developers to assign rewards based on the average operator price and consumption estimations to motivate the miners to support the applications.

Another purpose of the consumption assessment is to prevent the users in the CC from coding the wrong programs to result in an infinite loop that consumes the CC network resources. Developers need to pay before the business logic can be implemented.

◆ Auto Execution

Once the business logic is written into the network, unless all parties in the contract agree to terminate the logic, it is automatically executed. This is the advantage of decentralized system. For example, a trust whose beneficiary is the trustee's children, manages the property to the children after the age of eighteen years. This logic is very easy to write and execute on the CC.

◆Compliance with Legal and Compliance

Nikosabe first proposed the concept of the smart contract in 1990, but it has not been practically used due to the lack of a credible execution environment [21]. CC network is a trusted decentralized platform. In an interview, Mary Juetten [22] proposed the concept of Contract as Code, or "contract as code." As we design and develop the code, we will consider how to make the code more legally readable and add the "Intention to be legally bound" statement.

Due to the complexity of legal compliance provisions, we might consider specific local laws and regulations to design different versions of the script languages. We strive to make the code itself legally readable. We know this is a very challenging target, but as a bridge between the blockchain world and the real legal world, the compatibility with the legal and compliance is a very interesting direction.

We also anticipate the possibilities of the regulations changes frequently. In particular, CC adds a legally and compliance layer that interprets the codes and generates legal documents that are stored on the chain.

◆Easy to Use

We will develop the toolkits for developers to do debugging work. At the same time, developers can also find quick development templates in the stores to speed up the development progress.

◆Privacy Protection

CC can write the summary of the "witness" obtained from the hash function into the public chain. CC can also write the commercial logic into the public chain after encrypting it.

3.2.2 CC Application Store

Similar to Apple's App Store, apps are first reviewed by the regulators and then taken to the app stores. Regulators will also assess the quality of the product, efficiency and user’ s feedbacks,. They will decide whether to keep the apps in the store or remove them.

It is worth mentioning that the legal compliance supervisor can examine whether any application can be launched as a CC supervisor and check whether the application and the target user meet the current regulatory requirements.

3.3 CC Virtual Machine

The concept of a virtual machine comes from the abstract description of the computer resources based on the public chain and nodes. Virtual machines support and run CC business logic by consuming their resources. The services includes the codes, applications, clearing and data processing, and more. The virtual machine will also have a certain amount of the rewards to do so.

Because each network node on the CC network needs to compete to be the VM within a time slot, so which node would be the VM for that timeframe is not certain. It's so called as a virtual machine.

The virtual machine allocates resources owned by the virtual machine itself based on the computer resources and rewards consumed by the application. Here we borrow the definition from EOS.io [18], the computer resources: CPU, hard disk space, memory and network bandwidth.

3.4 Case Study of the Applications

Let's take a few examples of how to use CC to develop financial applications. We use solidity grammar expressions as the coding sample to demonstrate the programming logics. It does not mean that CSSL will use this expression.

3.4.1 Codes for Debt Originations

Bond issuance process can be more complicated, but the core content is to define the number of bonds, the transfer of the bond, as well as the destruction of the bond after maturity. If considering issuing a bond on the CC, the core logic can be written in this:

```
1 pragma cssl ^0.0.1; // declare the version

// line 2 to 22, defines a bond contract, named as MyBond
// line 3 to 7, defines some public variables such as name of the bond, total
supply, bond transfer and destruction of the bond.

2 contract MyBond {

3     string public standard = 'Bond 0.1';
4     uint256 public totalSupply;
5     mapping (address => uint256) public balanceOf;

6     event Transfer(address indexed from, address indexed to, uint256 value);
7     event Burn(address indexed from, uint256 value);

// line 8 to 11, defines the initial supply of the bond.

8     function MyBond(
9         uint256 initialSupply
      ) {
10          balanceOf[msg.sender] = initialSupply;
11        totalSupply = initialSupply;
    }

// line 12 to 17, defines how to transfer a bond from one to another

12    function transfer(address _to, uint256 _value) {
13          if (balanceOf[msg.sender] < _value) throw;
14          if (balanceOf[_to] + _value < balanceOf[_to]) throw;
15          balanceOf[msg.sender] -= _value;
16          balanceOf[_to] += _value;
17          Transfer(msg.sender, _to, _value);
    }

// line 18 to 22 defines how to destroy the bond after maturity

18    function burnFrom(address _from, uint256 _value) returns ( bool success ) {
19          if (balanceOf[_from] < _value) throw;
20          balanceOf[_from] -= _value;
21          totalSupply -= _value;
22          return true;
    }
}
```

3.4.2 Letter of Credit and Trade Finance

Here is a sample for a letter of credit (L/C) works on CC. We can understand the letter of credit codes will be written similar to the bonds above. First of all: (1) The letter of credit has a three-way guarantee from two banks, which require the digital signatures. We can have the financial institutions sign it by calling a function from smart contract. (2) Then we need to implement an event-driven signal for the L / C, associated the L / C with a specific trade, or assets. (3) When a user makes a finance on this letter of credit, other financial institutions can easily verify whether the digital signature comes from a financial institution which is a guarantor.

04 Legal Compliance and Regulation Layer

Legal and compilation layer is a level of our CC that is specifically designed for the CC business logic translated to legal documents. In fact, similar applications and ideas are not uncommon in the financial industry. For example, when dealing with derivative products in the financial industry, front office staffs usually confirm the trade with a simple term-sheet. The term-sheet usually is a list of variables with economic terms. The banks use the phone, email , fax or other method to confirm the front office terms. And the back office staff will generate the legal contract according to the front office terms, also known as back-office confirmations.

We borrow the above idea to generate the legal documents from CC business logics. Our current thinking is to use two different systems to achieve this job.

4.1 the Bella, A.I. Experts System

First of all, we introduce the first system "Bella", is an expert system [23]. We will use the code template and the legal template. We will do the mapping between these two templates: mapping their variables to the corresponding template. When writing the codes, developers choose to use legal compliance template by the expert system, the definition of variables will be limited by the template definition, including but not limited to the size, range, access to information and many other features. The benefit of doing this is that the quality of the legal document is high. The disadvantage is that we need a lot of template to cover most of the business and it is not very flexible.

4.2 the Lyra, Deep Learning and Neural Network

The second system, "the Lyra," will use deep learning and artificial neural networks to learn from a large number of samples and automatically generate legal contracts from the codes. The benefits of doing so are obvious: it is automatically adapted to a variety of business logic and codes. The disadvantage is that the quality of generating a new legal documents might be unstable.

We may use one of the above two methods or a mix of two methods to generate legal documentations. We are aware of the current challenges from semantic

identifications and the artificial intelligences. But when the design combined with our CSSL language, it is possible to generate "continuous" and "smooth" changes of documents. We think this will be a very interesting unknown area to explore.

05 Data Storage Layer

In the CC, there are several types of data that the data storage layer will process: user data, code data, legal documents, settlement data, and Celes Chain's token and ledgers, and etc.

The user group data is the KYC (Know Your Client) data for all users as well as various types of authentication and signatures. Such critical privacy is typically stored by the application developer and encrypted, to the local database. They could use the CC's public database for a hash "witness" on the chain.

Various types of code data including the code itself, procedures, contracts, functions, applications, templates and business logic, can be encrypted and stored in a local or public database. One can also store the encrypted data directly on the chain, depending on the value of the code. For example, public information like templates can be placed in a public database, leaving a "witness" on the chain.

The data / documents generated by Legal and Compliance Layer is generally a legal document associated with digital signatures. This part of the data is similar to the codes, according to the value, it would be the developer’ s choice for the public database or the public chain as the "witness."

All types of settlements data and Celes Chain's tokens ledger data are stored on the public chain to meet the decentralized requirements.

A "witness" is a hash "summary" of a piece of information using a hash function. Because the hash function is a one-way function, and irreversible [24]. This "abstract" can be saved on a public chain as a witness. Anyone can verify it with the original text, but can not restore the original text without the original text itself.

06 Consensus Layer

This protocol uses the time division multiple proofs protocol (TDMPC) [1]. In TDMPC, the note uses PoW to obtain the wood and uses PoC to generate tokens and produce blocks asynchronously. This allows the CC to get a better balance between decentralization and efficiency, and gives the miners enough incentives to invest in stable hardware resources to make CCs more efficient and stable to support applications.

PoW, also known as Proof of Work [25], is a consensus algorithm that one computer one vote to elect the block producer. The method of voting is to calculate the hash function to prove that the note with faster computer can produce the block..

PoB, or Proof of Burn, [26] is a method to vote for who will produce the block by burning their own tokens. The greater the number of the burn tokens, the greater the probability of getting the right to produce the block.

6.1 TDMPC and Efficiency

Here we refer to the paper [1] of TDMPC, a brief description of the proof procedure that the efficiency of time-division multiple proof protocol is higher than that of PoW. We first define the power of any one node as follows:

$$M=m_1+m_2 \sim(1)$$

m_1~Node's total resources invested in mining
m_2~Node's total resources invested in system to run applications
M~Node's total resources invested in mining and system to run applications

Then we can get any one of the node's mining yield is as follows:

$$Return = -b/(P\cdot C)\cdot m_1^2+((M\cdot b)/(P\cdot C)+a/P)\cdot m_1$$

P~total mining resources within the system
C~total applications

〖m_1〗 _ /P~expected mining hit ratio
a~fixed rewards from mining
b~ rewards from running applications

Since the rate of return is a negative quadratic curve with m1 as an independent variable, there must be a m1 that maximizes this rate of return. We can conclude that when any node spent all its resources to mine rather than increase its hard-ware resources, the node can maximize the benefits. Therefore, in an ordinary PoW system, because the mining machine has no incentive to invest in computer hardware resources, it is not able to run a stable application on a large scale.

On the contrary, if you remove the fixed income mining, then any miners must configure the ratio of 1: 1 mining / computer hardware resources in order to achieve maximum mining revenue.

6.2 CC Consensus Module

CC consensus uses TDMPC. As shown in the figure below, PoW, a slower proof of work, is used to generate wood for burn. Then, PoB was used to speed up incineration (PoB), and CC coins were excavated by burning the wood as a bonus as well as producing the blocks.

From Chapter 6.1 and the TDMPC theory, we know that blockchain networks can run large-scale applications when PoW + PoB proves that all token rewards obtained from their burning come from their supported applications. In our CC, the miners can not get fixed income. If the value of CC becomes higher, external hash power can be indirectly rewarded via PoW and obtain the tokens. This demonstrates the true decentralization. Due to the speed of obtaining the woods and the speed of obtaining the tokens are not the same, PoB can be used to produce tokens and generate blocks at higher speed. In other words, the plat-form based on this, it can be used for large-scale applications and is efficient.

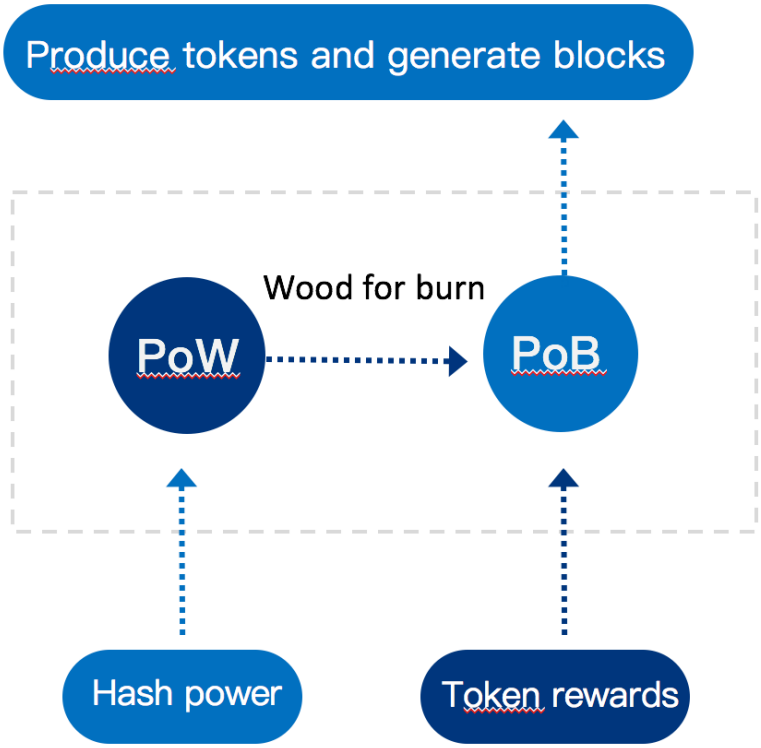

Figure 3 – CC Consensus Module

07 Usage of Token Products and Ecosystems

7.1 Usage of Token Products

Users who have the tokens can choose the following three strategies (as shown)

Use Strategy 1: Buy CC Services and Applications
Use Strategy 2: Purchase External Hash Calculations (If Available) with tokens and then obtain the tokens Indirectly
Use Strategy 3: Get Profits by Purchasing CC Services, Purchase external hashing power (if any) by fiat money, and obtain tokens Indirectly.

Users use their own strategy for their most profitable tactic, allowing them to monetize through arbitrage and value-added through such arbitrage.

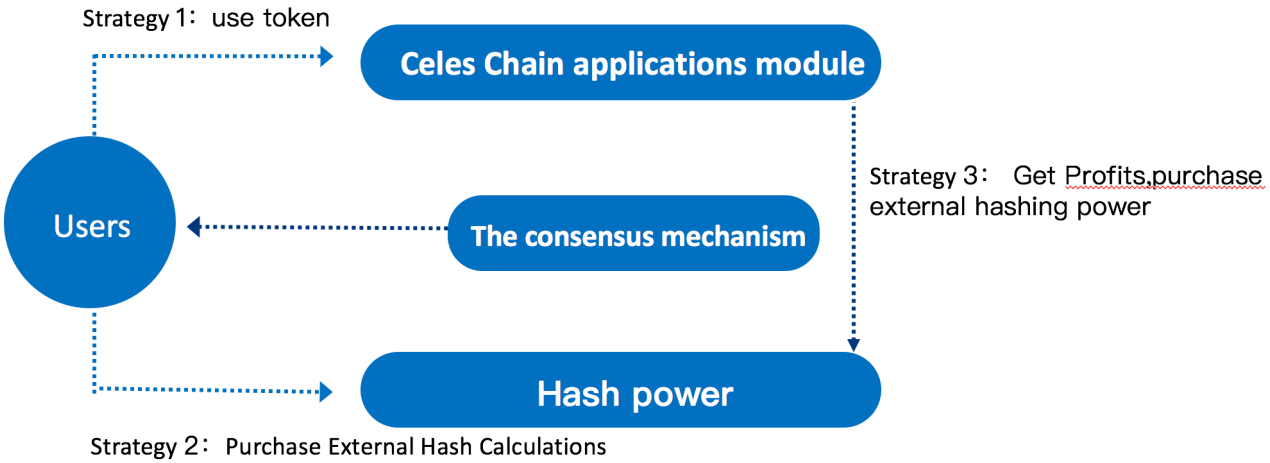

Figure 4 Usage of Token Products and Ecosystems

7.2 Ecosystem

Hash power input into the consensus mechanism and produce block to support CC applications. As shown in the figure, a bonus coin is dispensed into the application module and entered into the token collection. CC system to collect the tokens as a reward put it back into the consensus mechanism to maintain CC network. Earlier private crowdfunding tokens as the initial tokens are issued into the application system.

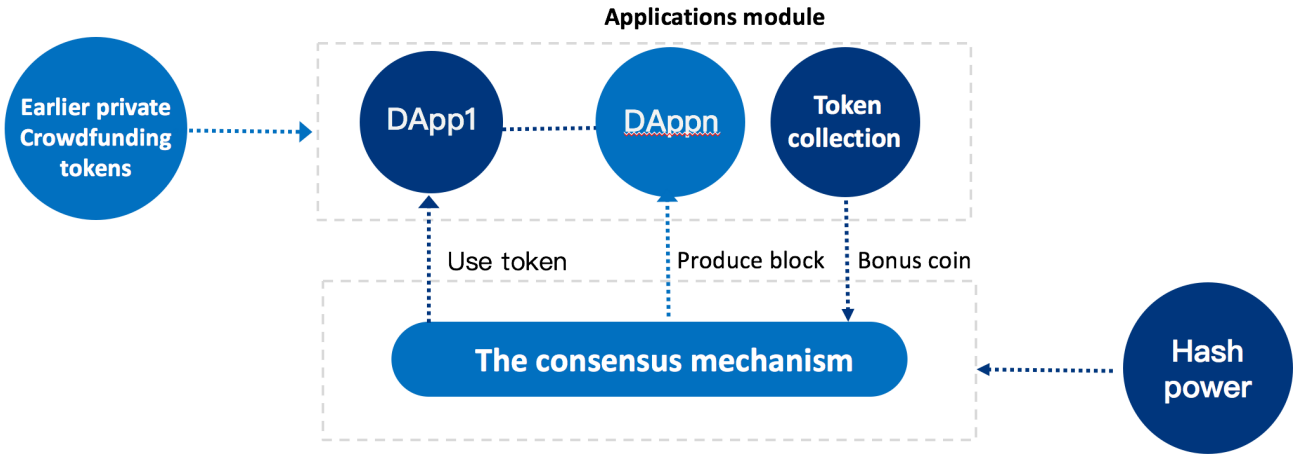

Figure 5 Ecosystem

08 Conclusions

Celes Chain uses decentralized consensus and blockchain technology to support various types of financial applications to create the "Wall Street" on the block-chain. We are the solution to the reduce the current regulatory enforcement costs and restore the "confidence" in financial markets.

At the same time, we use TDMPC protocol [1], which is a good balance between "decentralization" and "efficiency". This consensus enables our CC technology platform to enable our miner to have enough power to maintain hardware re-sources for CC applications. In addition, we will be developing a powerful, intui-tive, concise and scripted language for our financial applications. Various types of participants on the CC platform can leverage powerful CCSL to assemble their own financial and business logic and develop applications. At the same time, regulators can regulate applications, datas and user activities according to the law. In addition, we compile some of our agreements, applications, code, and data into a text that meets the legal specifications to facilitate further com-pliance and regulation.
Finally, the data, contracts, and related information for these applications will be "recorded" in encrypted form into the "consensus" chain to ensure that these "records" are not tampered or illegally captured. Ultimately, Celes Chain can attract regulators, financial institutions and end-users alike by reducing opera-tional costs and increasing regulatory efficiency.

10 Citation List

【1】Yeung (2018), Time Division Multiple Proofs Consensus Protocols, working paper
【2】Nick Szabo, Smart Contracts, 1994, http://www.virtualschool.edu/mon/Economics/SmartContracts.html.
【3】John C. Bogle (2008), Commentary: Why we lost faith in Wall Street –– and what to do, CNN, http://www.cnn.com/2008/POLITICS/12/01/bogle.investors/index.html
【4】Ivana Kottasova (2016), $9 trillion and counting: How central banks are still flooding the world with money, CNN, http://money.cnn.com/2016/09/08/news/economy/central-banks-printed-nine-trillion/index.html
【5】Governor Daniel K. Tarullo (2016), Financial Regulation Since the Crisis, https://www.federalreserve.gov/newsevents/speech/tarullo20161202a.htm
【6】Philip Stafford (2018), Mifid II and dark pools: what are regulators up to?, https://www.ft.com/content/491bbfa8-f3ba-11e7-8715-e94187b3017e
【7】Volcker Rule, https://en.wikipedia.org/wiki/Volcker_Rule, wikipedia as of Jan 17,2018
【8】Peter Pham (2018), Why are banks too big to fail?, https://www.forbes.com/sites/peterpham/2018/01/15/why-are-banks-too-big-to-fail/
【9】Satoshi (2008) , Bitcoin: A Peer-to-Peer Electronic Cash System
【10】Leslie Lamport (1982), The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems
【11】Evelyn Cheng (2018), Second-largest cryptocurrency ripple may have run ahead of itself, CNBC, https://www.cnbc.com/2018/01/05/second-largest-cryptocurrency-ripple-may-have-run-ahead-of-itself.html
【12】Alex Hern (2018), Bitcoin's energy usage is huge — we can't afford to ignore it, theguardian, https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency
【13】https://www.reddit.com/r/ethtrader/comments/65nc7d/what_dapps-software_is_being_built_on_bitcoin/, taken at Jan 17, 2018
【14】http://www.businessinsider.com/the-worlds-2nd-largest-crypto-currency-ethereum-had-an-even-bigger-price-surge-than-bitcoin-2017-5, taken at Jan 17, 2018
【15】https://www.ethereum.org/
【16】Banks tap Ethereum smart contracts for MiFID II compliance, https://www.finextra.com/newsarticle/31465/banks-tap-ethere-

um-smart-contracts-for-mifid-ii-compliance/blockchain
【17】http://www.ibtimes.co.uk/ubs-barclays-credit-suisse-thomson-reuters-explore-ethereum-based-mifid-ii-solution-1651014, taken at Jan 17, 2018
【18】https://github.com/EOSIO/Documentation/blob/master/Technical-WhitePaper.md, taken at Jan 17, 2018
【19】https://www.reddit.com/r/ethereum/comments/6s6eh8/delegated_-proofofstake_vs_proofofstake_also_im/, taken at Jan 17, 2018
【20】Securities and Exchange Commission, July 25, 2017, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO
【21】Josh Stark (2016),https://www.coindesk.com/blockchain-smarts-contracts-real-world-law/
【22】Mary Juetten (2017), https://www.forbes.com/sites/maryjuetten/2017/08/16/legal-technology-and-smart-contracts-contract-as-code-part-i/#15f7dd6a8b24
【23】赵南元 (2002), 认知科学揭秘（第二版）
【24】http://www.aspencrypt.com/crypto101_hash.html, taken at Jan 17, 2018
【25】https://en.wikipedia.org/wiki/Proof-of-work_system, take at Jan 17, 2018
【26】https://en.bitcoin.it/wiki/Proof_of_burn, taken at Jan 17, 2018
【27】https://en.wikipedia.org/wiki/Markets_in_Financial_Instruments_Directive_2004, taken at Jan 28, 2018
【28】Counting the cost of MiFID II, IHS Markit, 2018
【29】http://finance.sina.com.cn/stock/usstock/c/2018-01-03/doc-ifyqcwaq7305911.shtml, taken at Jan 28, 2018
【30】http://thehill.com/regulation/finance/288391-report-puts-cost-of-dodd-frank-at-36b, taken at Jan 28, 2018
【31】https://thinkprogress.org/5-numbers-to-know-as-dodd-frank-wall-street-reform-celebrates-its-5th-birthday-e145f4360b7c/, taken at Jan 28, 2018
【32】https://www.reuters.com/article/banks-volcker/u-s-volcker-rule-may-have-less-impact-on-bank-revenues-than-expected-idUSL2N0JS0BZ20131218, taken at Jan 28, 2018
【33】https://en.wikipedia.org/wiki/Turing_completeness , taken at Jan 28, 2018

Disclaimer

The user expressly knows and agrees that the user is using the CC platform at the user's sole risk.

The user acknowledges that the user has an adequate understanding of the risks, usage and intricacies of cryptographic tokens and CC open source software, CC platform and CC

The user acknowledges and agrees that, to the fullest extent permitted by any applicable law, the disclaimers of liability contained herein apply to any and all damages or injury whatsoever caused by or related to risks of, use of, or inability to use, CC or the CC platform under any cause or action whatsoever of any kind in any jurisdiction, including, without limitation, actions for breach of warranty, breach of contract or tort (including negligence) and that neither CC (i.e. CC) nor CCteam shall be liable for any indirect, incidental, special, exemplary or consequential damages, including for loss of profits, goodwill or data that occurs as a result.

Some jurisdictions do not allow the exclusion of certain warranties or the limitation or exclusion of liability for certain types of damages. Therefore, some of the above limitations in this section may not apply to a user. In particular, nothing in these terms shall affect the statutory rights of any user or exclude injury arising from any willful misconduct or fraud of CC.