

# How To Build A New Web3.0 Financial Market

Li Li (Combox DAO LLC)

[paul.lee.combox@gmail.com](mailto:paul.lee.combox@gmail.com)

## Abstract

Most modern property exists as book-entry assets, which form the foundation of commercial activities. Moral hazard has long been a persistent issue in these activities, but the advent of blockchain and smart contract technologies offers a promising solution. That is to use the blockchain to record property rights and use the smart contracts to automatically control legal acts, so that: (1) right holders can directly exercise rights; (2) obligors have no chance to violate; (3) legal acts are fully disclosed in real time. This approach eliminates human intervention in commercial activities, addressing issues such as minority shareholder protection, insider control, misleading disclosures, and potentially eradicating moral hazard altogether.

Removing human intervention through automated control, replacing trust in traditional centralized entities with trust in a temper-resistant rigid code, and establishing a credit system based on a distributed system and rigid code is the meaning of 'Decentralization' and, in fact, the core reason for the success of Bitcoin. In cash payment scenarios, the goal of 'Decentralization' is relatively easy to achieve because of the simplicity of the legal relationship and the singularity of the act. Can the same be achieved in other more complex business scenarios?

With reference to the 'Turing Machine' model, this paper aims to create a general-purpose computational model for the automatic control and recording of book-entry assets and commercial legal acts. The system consists of three types of smart contracts: (1) Registers are used to define the three types of data objects: property certificates (for property rights), economic organization roles (for governance rights) and documents of intention expression (for the track records of legal acts); (2) Code of Conduct is used to define the system of rules to be followed by the legal acts;

(3) Keeper of Books is used to define specific algorithms and operational processes of the legal acts in the two-step process of condition validation and consequence realization.

Based on the concept of "Code Is Law", the above model can be extended and applied to a wider range of commercial fields such as stocks<sup>1</sup>, bonds, loans, notes, trusts, funds, factoring, leasing and so on. In this way, we can gradually build a new financial market in the sense of Web3.0 with the feature of exercising of legal rights in "self-service" mode.

## 1. “Moral Hazard” and solutions

As human civilization enters the 21st century, the vast majority of wealth exists in the form of book-entry assets, such as bank deposits, stocks, bonds, real estate, intellectual property rights, fund units, trust beneficiary rights, bills of lading, financial instruments and so on. To define the rights and interests in these assets, identify their holders, and regulate trading activities, various laws, regulations, charters, and contracts have been established.

However, in the real world of business, rules and commitments are often violated. Minority shareholders' rights to information and voting are often suppressed because administrators only take the orders from the majority; trustees may breach their fiduciary duties by harming the beneficiaries through overpriced related transactions; and management may mislead investors by disclosing false information.

The common thread in these failures is that right holders cannot directly exercise their rights or achieve the intended legal outcomes. The right holder has to work through an agent or trustee to exercise their right, or needs the cooperation of the obligor to

---

<sup>1</sup> This model has been implemented in the ComBoox platform (<https://comboox.vercel.app>) for equity transfer and corporate governance, demonstrating its feasibility in automating sophisticated legal acts.

achieve their business purpose. If the agent, trustee or obligor maliciously breaches the rules or commitments, the rights and interests of the right holder will be harmed. This phenomenon is known as the moral hazard problem.

How to solve this problem?

The emergence of blockchain technology offers a new solution. That is using the immutable distributed ledgers to keep the book-entry records of properties, and using smart contracts to automatically control the entire process of legal acts. Then:

- (1) agent, trustee, or any other intermediaries can be completely removed from the exercising process of legal rights;
- (2) claims that require the cooperation of the obligor will be transformed into property disposal rights that directly changes the state of the book-entry assets; and
- (3) legal acts and information disclosure will no longer be two separate behaviors and will have no logical difference or time lag.

In brief, by introducing an automatic book-entry model based on blockchain technology, the business and financial activities can evolve to a new level:

- (1) right holders directly exercise rights;
- (2) obligors have no chance to violate; and
- (3) legal acts are fully disclosed in real time.

"Code Is Law". People can rely on the automatic execution of rigid code to achieve business purposes, no longer relying on the trust of the centralized entities, based on distributed systems and rigid code to establish a credit system. This is the meaning of 'Decentralization', in fact which is also the core reason for the success of Bitcoin.

In cash payment scenarios, the goal of "Decentralization" is relatively easy to achieve, because the legal relationship is simple and the content of the legal act is uniform. Can this objective be achieved in other more complex commercial scenarios?

## **2. “Turing Machine” and commercial activities**

The 'Turing Machine' model, proposed by the great mathematician Alan Turing, is a formal computational framework that describes the execution of algorithms through states, rules, and functions. In theory, all computable problems can be automatically controlled by computers through this model. The key to its implementation lies in three points: (1) defining a finite set of states; (2) determining a system of rules for state transition; and (3) defining a specific algorithmic process (i.e. a transition function) for state evolution.

### **2.1 States**

All commercial activities revolve around property. Whether it is buying, selling, lending, renting, licensing, mortgaging, pledging, assembling property to form an economic organization (e.g. a company or a partnership) or establishing a trust, the core purpose, object of disposition and vehicle of rights of these commercial activities are almost always related to property.

Most modern property exists as book-entry assets. Registers document rights holders, quantities, boundaries, interests, and encumbrances of these assets at different points in time, creating distinct asset states over a timeline. The concepts describing these asset states—such as property rights, claims, intellectual property, corporations, partnerships, trusts, banking, finance, and securities—are rooted in commercial law.

### **2.2 Rules**

In order to regulate commercial activities, laws and regulations have been enacted, and charters and by-laws have been concluded. These code of conduct and institutional rules, on the surface, are to regulate people's commercial behavior, but in a more essential level or in terms of their original intention, are to define the transition rules for the assets on their states, which reflects people's expectations on the certainty outcome of the states transition. Therefore, laws,

regulations, charters and by-laws essentially define or reflect the system of rules that must be followed for the asset states transition.

### **2.3 State Transition Process**

Commercial activities, in other words, commercial legal acts, are the processes by which people dispose of property rights and cause changes in the state of property rights. Specifically, buying and selling are the process of changing the owner of the property in exchange for consideration; lending and leasing are the process of changing the user of the property temporarily in exchange for interest; mortgage and pledge are the process of temporarily freezing the disposal rights of the property to guarantee the realization of the creditor's rights; establishing a company is the process of changing the owner of the property in exchange for the governance and beneficiary rights of the economic organization. These commercial acts will all lead to changes in the state of property and the said "legal and compliance", means that commercial acts should comply with the predefined rules, so as to achieve the certain outcome of state transition.

Therefore, book-entry assets and their related commercial legal acts satisfy the basic consisting elements of the "Turing Machine" model, and can certainly build an automated system with state, rules and transition functions as elements to implement automated control by computer.

Certainly, analogy is not a rigorous reasoning, and the above discussion is not intended to prove that all commercial legal acts can achieve automatic control. What's more meaningful is that to achieve automatic control of limited legal acts through predefined rules and systems, so as to achieve the goal of excluding human intervention and eliminating moral hazard in specific fields and specific scenarios of commercial activities.

### 3. System Architecture

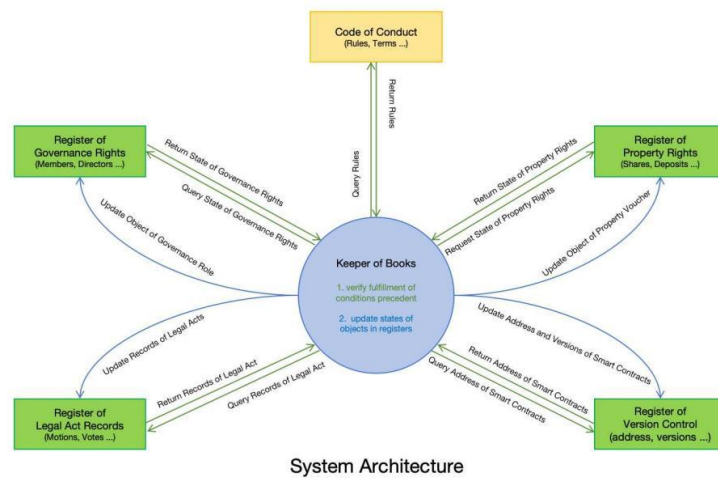
Book-entry assets are essentially property rights recorded in the form of states. Governance rights in economic organizations are decision-making and voting rights obtained by members through the exchange of property rights. The legal rights involved in commercial activities mainly fall into these two categories.

Legal acts are the process of exercising legal rights, and their results will lead to changes in the state of legal rights. Legal rights are both the source and basis of legal acts and the disposition objects thereof. Legal acts need to follow codes of conduct, including universally applicable legal norms and charter rules that take effect within specific economic organizations.

In commercial activities, two types of information must be recorded: the attribute states of Legal Rights and the contents of Legal Acts.

The Legal Rights can be further categorized as property rights to possess, use, benefit from and dispose of the subject assets (the “**Property Rights**”), and the governance rights derived from the constitutional documents of the economic organization concerned, such as information access rights, decision-making rights and voting rights (the “**Governance Rights**”).

In terms of code implementation, Property Rights can be defined as data objects representing their legal certificates, such as "stock" or "bond". Governance Rights can be defined as data objects representing specific roles in the organization, such as "member" or "director". As for contents of Legal Acts, they can be defined as data objects describing the documents of Intent Expression (the “**Intent Expression**”), such as "voting ballot" or "trade order". In this way, Legal Acts will be transformed into unilateral acts of exercising legal rights, and the consequences of which will be directly implemented as creation, updating or deletion of certain data objects recorded on the block chain.



The automated book-entry system consists of three types of smart contracts: (1) Registers; (2) Code of Conduct; and (3) Keeper of Books.

### 3.1 Registers

They record the states of Legal Rights and the contents of Legal Acts, and can response queries for these data in real time. For example, a smart contract named “Register of Shares” can be used to record the states of the Property Rights object “Share Certificate” so as to track the attributes of the shares represented on it in terms of the class, sequence number, par value, shareholder, acquiring price, voting weights and etc. Another smart contract named “Register of Members” can be used to record the states of the Governance Rights object “Member” so as to track the attributes of the Member in terms of its account address, and shares in hand. A smart contract named “General Meeting Minutes” can be used to record the Intent Expression object “Vote Ballot” so as to store the contents of the ballot in terms of the voter’s address, voting time, attitude, and voting weight. And, a smart contract named "List of Orders" can be used to record the "Trade Order" data object to record the order information such as buy or sell direction, underlying stock class, intended price, quantity, margin amount, expiration date, and other relevant attributes.

### **3.2 Code of Conduct**

It defines the static parameters of rules regulating the legal acts, and can response the queries for rules in real time. For example, in the field of corporate governance, for the voting rule of “regular issues of General Meeting shall only be approved upon consents of members holding at least 50% of total voting weight”, “50%” can be set out in the Code of Conduct as one of the static parameters of voting rule for regular issues of General Meeting. In the votes counting stage, this parameter will be retrieved from Code of Conduct so as to compare with the actual voting results. If the aggregate voting weights held by the supporting members is more than 50%, the motion concerned will be passed, otherwise be rejected.

### **3.3 Keeper of Books**

It controls the entire process of each Legal Acts, which essentially consists of validating the preconditions and realizing the consequences in two sections. Preconditions of a Legal Act include (but not necessarily fully covers) three kinds: (1) Access Control condition based on the account address of message sender; (2) Time Restriction condition based on the current block timestamp; and (3) Legal Logic Restriction condition based on the current state of certain data objects. Legal Logic Restriction is the most complex of the three types of conditions, which needs to be based on the specific scenarios of legal act, applicable rules, business intentions for customary settings and formal abstraction, essentially reflecting the thinking logic of commercial lawyers. Realizing consequences operations mainly refers to calling the specific write functions of the relevant Register smart contracts so as to create, update or delete the data objects concerned.

In order to ensure that the write commands, which are able to change the state of the relevant smart contracts, can only be invoked by the specific external accounts or be triggered by the specific contract accounts, some access control technical measures shall be taken (such as inherit certain access control smart contracts) in the deploy or initiation process.

Once deployed, the computational logic and operational processes of a smart contract's functions cannot be altered. Meanwhile, in order to keep the stability and consistency of the governing rules of Legal Acts, the static parameters of rules in the Code of Conduct can no longer be revised after its conclusion. If the calculation logic or operation process of a deployed smart contract is intended to be revised, or the rule parameters in the Code of Conduct are to be amended, a new version of smart contract will have to be deployed to replace the old one. In order to manage different versions of the same type of contract, a special Register for version control can be deployed to categorize the contracts' address according to their versions and types, and to indicate whether the legal status of the relevant contract is "Effective" or "Expired". This will facilitate to search for data in the historical contracts, and, on the one hand, will also be helpful to establish a closed-loop upgrade mechanism within the system.

#### **4. Implementation Method**

Based on the above system of smart contracts, the implementation method for automatic book-entry can be arranged in the following steps:

##### **4.1 System Initiation**

Once the relevant smart contracts are developed, they must be deployed onto the blockchain network. And, some fundamental data shall be input into the relevant smart contracts to form the initial state of the system. Moreover, some access control configuration shall be set up so as to ensure: (1) the edit right to the Code of Conduct is revoked (transfer to Zero address) to fix the contents of the rules; and (2) the write functions of Registers can only be triggered by the Keeper of Books.

##### **4.2 Command Receiving**

The Keeper of Books receives a transaction call for a specific Legal Act, initiating a precondition validation process and legal consequence realization process predefined in that function. The Keeper of Books shall be designed under the

basic concept of “process-oriented”, setting up the Application Programming Interfaces for each of the Legal Acts respectively as an independent process. Therefore, after receiving the transaction call, it will execute the calculation logic and operation process in a top-to-bottom order for the two basic sections of precondition validation and legal consequence realization.

#### **4.3 Preconditions Validation**

The Keeper of Books validates that all the preconditions for the particular Legal Act are fulfilled in accordance with the predefined validation process and algorithm. The transaction command will provide the address of the message sender, as well as the input key for retrieving the rule parameters and data objects. The validation algorithm generally requires three types of parameters to be retrieved as inputs from the system: (1) the static parameters of the relevant rules that serve as the judgement criteria; (2) the current block timestamp representing the state of time; and (3) the attributes of the particular data objects representing the state of Legal Rights or the contents of Legal Acts. Once these input data are obtained, the Keeper of Books will execute the validation algorithm to verify whether all the conditions are fulfilled one by one, and will terminate the process by returning an error message if any of the conditions are not fulfilled.

For example, during shareholder voting, the 'cast vote' function of the Keeper of Books validates preconditions as follows: (1) the Register of Members will be firstly called to verify whether the message sender account has the role of Member, and if so, the Access Control validation will be passed; (2) the General Meeting Minutes will be called to query the voting window of the specific motion, and then the timestamp of the current block will be retrieved, and if the current timestamp falls within the voting window, then the Time Restriction validation will be passed; (3) the General Meeting Minutes will be called to query whether the procedural state of the specific motion is “Proposed”, and if it is, then the Legal Logic restriction validation will be passed.

#### **4.4 Consequences Realization**

The Keeper of Books, in accordance with the predefined operation process, calls the relevant write API of the particular Register to create, update or delete the particular data object, so as to realize the consequences of the Legal Act. There are two kinds of intents of Legal Acts, one is to dispose Property Rights, and the other is to exercise Governance Rights. The legal consequences of the former will be implemented in the change of the state of book-entry assets, and those of the latter will be realized by recording the contents of the intent expression, or change of the state of assets or roles. For example, the legal consequence of paying book-entry assets will be implemented as a change in the holder of those assets, and the consequence of casting a vote will be realized by recording the voter's attitude and voting weights in the system. Some Legal Acts such as placing a trade order or signing a share transfer agreement, are slightly more complicated: they are Intent Expression for conditional trading assets. On one hand, the content of the Intent Expression needs to be recorded; on the other, a special automatic trigger mechanism needs to be set up to dispose of the subject assets automatically when the conditions are met.

Still taking shareholder voting as an example, after verifying the preconditions, the "vote" function will execute the following operations to achieve the legal consequence: (1) the Register of Members will be firstly queried for all the sequence numbers of shares held by the calling member; (2) according to these sequence number, the Register of Shares will be called for retrieving and calculating the aggregate voting weights of all shares held by the calling member; (3) the "cast vote" function of the General Meeting Minutes will be called, and the motion's number, member's number, the total voting weights it held, and the voting attitude will be written and stored into a newly created data object "Voting Ballot".

While, under certain circumstances, a Legal Act intended to dispose Property Rights may result in an update to the data object representing Governance Rights, and vice versa. For example, in case a member sells all its shares, at the same time when the holder of its shares is updated to the buyer, the seller is also

removed from the Register of Members and lose its role as a member. Moreover, if a resolution of the General Meeting is to pay a certain amount of cryptoassets to a third party, and the authorized executor executes this resolution on behalf of the company, then, such Legal Act will simultaneously update the state of the motion as “Executed” and also change the beneficiary of the amount of crypto assets to the account of the specific payee.

This is because the economic organization that generates Governance Rights is established by collecting property (or Property Rights) from its members. So, Property Rights are the basis and source of such Governance Rights. And since the purpose of such economic organization is generally to make profits, it determines that the decision issues of Governance Rights will be directly or indirectly relevant to the disposal of property (or Property Rights).

When upgrading the version of a specific contract in the system, in order to maintain the data of the historical version and to identify the currently valid version, the Keeper of Books will call the specific API of the Version Control Register to record the address of the new version under the relevant category in its contract address mapping table, and then set the state label of the new contract to “Effective”, and revise the state of the old version to “Expired”. This is a special operation for system maintenance purpose other than realizing the consequences of regular Legal Acts. However, if the contract to be updated is a Code of Conduct, it is tantamount to an amendment to the company's by-laws or to the regulatory rules of an authority, which has special commercial legal significance.

## **5. Summary and Conclusion**

With reference to the "Turing Machine" model, this paper essentially creates a general-purpose computational model for automatically recording book-entry assets and Legal Acts. It takes full advantage of the programmable attributes of smart contracts to implement and automatically control Legal Acts around book-entry assets with transparent, verifiable and rigid code, thus eliminating, to the greatest extent possible, the moral hazard caused by human intervention in commercial activities.

The difficulties and key points in applying the model lie in: (1) abstracting different assets or Legal Rights into data objects, (2) figuring out key parameters of legal rules to be followed from the laws, regulations or constitutional documents; and (3) analyzing, simulating and transforming the constituent process of each Legal Act (in terms of identity verification, conditions validation, rights exercise, and consequences recording) into automated operations of computer codes (for data retrieval, logical judgement and data updates).

In the process of building a new mechanism, the peoples will certainly face some difficulties and challenges. But none of these should be a reason to deny the evolution. Identity issues such as AML and KYC can be fully resolved during the account registration process by establishing a mapping relationship between the social identity and the public key address of the e-wallet. This does not conflict with the current KYC process for opening stock accounts or registering financial market users. As for the security vulnerability of smart contracts and the problem of adapting the financial regulatory system of different jurisdictions, it is essentially a problem of the rigor of the business and legal logic of smart contracts, which needs to be gradually improved through continuous practice, testing and system upgrading. Openness and public disclosure of smart contract source code is the best way to eliminate system loopholes. Relying on the oversight power of the whole society to correct the errors and omissions is the same reason as correcting the omissions through public comments in the legislative process.

Although Real World Assets are diverse and their transaction modes vary widely, with the support of "Turing-complete" programming languages, smart contracts can definitely be used in limited commercial areas or scenarios to implement automated control. Automated means standardization, and distributed means public disclosure. These characteristics are very suitable for the financial and securities market, which emphasizes standardization and transparency.

If the above model can be applied to finance and securities, then: (1) financial regulation and dispute resolution will shift from ex-post behavioral supervision and breach remedy to ex-ante smart contract verification; (2) payment-versus-delivery, real-time settlement, and continuous trading will become the regular practice in the

market, leading to a significant improvement in financial efficiency; (3) moral hazard issues such as minority shareholder protection, insider control, and misleading statements will be easily resolved.

By continuously expanding the application scope of the model, a "decentralized" credit system can be established product by product, field by field, thereby building a new type of financial market in Web3.0, characterized by the exercise of legal rights in "self-service" mode.

**(The End)**