Times Chain Whitepaper

Build to be boundless

Table of Contents

Abstract

Times Chain (referred to as Times) is committed to building a boundless blockchain world, founded in 2015. Blockchain now is considered as one of the technological innovations of the greatest potential and creativity in the world. There were three key turning points in the human history: The First Industrial Revolution, marked by machines replacing manual labor, the Second Industrial Revolution, followed by the inter-combustion engine and other mass production techniques, and the Third Industrial Revolution, driven by computer technology, nuclear energy, space technology and bioengineering. However, the foundation of our relations of production has remained the same: it is still confined into a centralized, top-down, pyramid structure. The more complicated this structure gets and the more levels it generates, the more difficult it is to ensure efficiency. Blockchain, also known as "the value network", is a decentralized and entrusted network that achieves peer-to-peer value exchanges. Times believes that blockchain technology is the innovation to reform the current relations of production and pave the way for the next long-awaited revolution in the history of mankind. With the help of Times, we can create a world where people are directly connected, trusted, collaborative, peer-to-peer-exchanged and value-driven under social consensuses.

Times will accomplish this goal in three phases. First, we'll build a secure and stable blockchain network with a modular design approach that will enable smart contracts and digital assets. Smart sandbox will also be used to create an environment for intellectual tests and monitors contractual execution. Sandbox ensures contracts are safe enough to avoid similar DAO incidents[1] before being uploaded officially to the chain. Second, we use forking to meet different business appeals such as insurance, document preservation, cryptocurrency, tracing, personal credit, and more. This phase will lead to an evolving, easy-to-use, low-cost, well-tailored blockchain network. Finally, through the Value Exchange Protocol (VEP), we will connect these forked and active networks together, and even open up data exchange with other networks (possibly non-blockchain) to build a connected and multidimensional data interrelated internet world. Using multidimensional data such as personal credit, assets, production and consumption data, community consensus, individual behavior, and value exchange will be better integrated organically. The token, named Times by Times Chain, holds the value of its ecosystem. Possessing Times gives you access to all basic blockchain services such as smart contract release, network forking, and much more.

Times is designed to put safety, stability and scalability in the first place in order to create the ecosystem mentioned above. Times, as a public chain, selects the more practical DPoS (Delegated Proof of Stake) consensus mechanism, which occupies less resource and creates a Result-delegated Proof of Stake (hereinafter referred to as RDPoS) consensus mechanism. Under the same security situation, RDPoS better improve the transaction performance of the entire network as well as other parameters of the network as a whole. Theoretically it has reached or even exceeded 1,000TPS (Transaction Per Second).

---

[1] https://en.wikipedia.org/wiki/The_DAO_(organization)

1   Background and Commitment

1.1 The history of network development

On Oct 29th, 1969, two separate points, ARPANET University of California at Los Angeles (UCLA) and Stanford Research Institute (SRI), successfully got connected through cable, signifying the arrival of the Age of Internet. In the last 50 years, with the emergent Internet based companies such as Amazon, Google, Facebook, Alibaba, etc., the information technology proved how it could change the world.

On Oct 31st, 2008, Satoshi Nakamoto presented the idea of Bitcoin in his essay, *Bitcoin: A Peer-to-Peer Electronic Cash System*, declaring the arrival of value transfer network. Bitcoin impressed the world by its anti-fraud, distributed-ledge, anonymous, and reliable characteristics. However, its performance and PoW (Proof-of-Work) consensus are yet to be improved. In recent years, groups and individuals have engaged in technical innovation on blockchain as trading performance, consensus algorithm and secure anonymity. For example, the Graphene tech and Lightning Network upgraded its performance; Proof of Stake (POS), Delegated Proof of Stake (DPOS) and Practical Byzantine Fault Tolerance (PBFT were proposed to refine its consensus algorithm; Zero-knowledge proof (ZKP and mixed-coin tech were expected to enhance security.

1.2 Why do we need blockchain?

Do we really need the blockchain? As an early participant and witness, Times believes that this innovation has an irreversible impact and will not be short-lived.

This is based on two reasons. First, we need real, valued information, that can reduce cost of trust. Computers and the Internet make information sharing cheaper and more convenient. With information technology, we can optimize the value chain and improve the efficiency of collaboration. However, we are aware of the faster and easier spreading of hazardous information and will prioritize the security over the cost of building a trusted network.

Secondly, we need a network to connect the social consensus, our behavior, and value incentives. We have witnessed only little changes in our relations of production: It is still a centralized, top-down, pyramid structure. The more complicated this structure gets and the more levels it generates, the more difficult it is to ensure efficiency.

Blockchain integrates distributed storage, encryption technology, P2P network and other technologies. It has the technological advantages of decentralization and trustworthiness, which is known as the value network. Blockchain will more efficiently solve problems of trust between people and create a new production network -- a peer-to-peer value exchange.

1.3 Topics of unsolved problems

Since its invention in 2008, Bitcoin has derived blockchain technology, and countless

technology enthusiasts have been contributing to the blockchain development. There have been the Ethereum, which serves as a decentralized platform, Bitcoin and Lite Coin, which focus on the development of digital currency, Factom, which provides filing of notarization, Zcash and Dash, which protect user privacy, Bitshare, which functions as a decentralized cryptocurrency exchange, and even Corda, R3CEV's popular distributed bookkeeping platform.

Despite the rapid development of the blockchain technology, there are still challenges ahead.

(1) Security risks of smart contracts. Users might lose their digital assets during hacker attacks.

(2) Difficulties of cooperations and interconnections of different blockchain platforms of different fields of application. Although such information interactions were already attempted, it is not sufficient to support the development of the whole blockchain ecosystem.

(3) Difficulties of linking between the blockchain world and the non-blockchain based reality. Ideas cannot be easily put into application, such as tracking of commodity authentication.

(4) At present, the blockchain industry still requires high technical qualifications, which leads to the high cost of large-scale business.

(5) Low transaction performance compared to the centralized systems.

1.4 Why do we need Times?

Times prioritizes security, stability, extensibility. By introducing cutting-edge designs of virtual machines, smart sandbox, value exchange protocal, and forking mechanism, Times creates an evolving, user-friendly, low-cost, and customizable blockchain network. The optimization of block interval, block volume and consensus algorithm also helps Times reach a performance rate of up to 1000TPS. Times believe that as the technological innovation creates a new production relation network, it will solve the problem of trust in interpersonal communications and organically integrate societal consensuses, individual behavior, and value exchange into an inseparable whole.

2 Principle

2.1 Stability

Network stability is essential to the functioning of a blockchain solution. This is, however, increasingly challenged by potential uncertainties, given the platform's decentralized nature and its ever-expanding number of applications. Times, with its philosophy of modular design and simplification, developed LVM (Lua Virtual Machine. The new VM, exclusively designated to smart contracts, offers two advantages. It has an upgraded performance rate powered by Lua language, effectively protecting against potential system coupling. And it also adopts a separately run and independently built structure to prevent the entire network quality from being affected by local hazards.

2.2 Safety

PoW used to guard the security of the Bitcoin network, but due to the increasing mining demands and hashing force, a significant amount of power has gone into the hands of miners and mining pools, resulting in an unwanted centralized "central server". If an entity controls 51 percent of the computing power, theoretically, it is possible to control the majority of Bitcoin transactions, which is known as DOS (denial-of-service attack. Besides, high power consumption also generates a huge cost.

Compared to the PoW model, the PoS (Proof-of-Stake model aims for a higher level of security and a wider range of applications. PoS model contributes to the network security only when attracting enough holders for PoS mining.

Based on PoS, DPoS was later released as an enhanced version; but Times even invented a more commercial-friendly and universally-accepted version, the RDPoS consensus mechanism. When run just as securely as DPoS, RDPoS can increase the block response and improve the stability and security of the network.

In addition, Times proposed a smart sandbox mechanism. Any released contracts should be test-run in the smart sandbox in the first place to be automatically tested in case of health deteriorate or loopholes. The network determines by itself if the newly written contract qualifies to be uploaded to the Times ecosystem.

2.3 Scalability

Scalability is proposed to solve the problem of incompatibility of blocks in the blockchain. First of all, we believe that upgrading and forking are the effective ways of network evolution. After fork occurs, it will generate a main chain and a number of sub-chains. All chains are completely equivalent in structure, but each is given a different logo based on different community consensuses. Each sub-chain can be customized according to different applications by constructing

the VEP (Value Exchange Protocol, which, like a gateway, allows information sharing and value exchanges among chains This kind of collaboration forms a multi-application network. Not only that, but the online data of non-blockchain based events will also be incorporated into the Times ecosystem. It is supplemented with smart contracts to respond to events in the real world.

2.4 Easy-to-use

Times provides with ease of use in two ways. The first is to provide the Blockchain as a Service (BaaS for short) to lower the technical threshold for enterprises and individuals. Blockchain applications become easy-to-use by the means of forking of chain, data customization, smart contract publishing and upgrading, asset transaction monitoring, and supplement with visualization. The second is the offer of multiple programming language support, from Lua, C++ to Java, that encourages most of developers and enthusiasts to involve easily.

3 Implementation

3.1 Smart contract & LVM

The conventional principle of smart contract only allows for data access within blockchain networks. However, Times rebuilds this technology into one that enables data interaction between the blockchain system and outside networks. This can also realize a synchronization between daily activities, such as business process or legal enforcement, and data status changes.

Business applications in reality are complex due to the nature of data structures and business rules and Times is making two aspects of preparation to overcome such complexity. The first is singling out abstract ideas and general requirements behind potential applications in order to accordingly design the API interface and data structure in advance. The second is selecting a Turing complete language to approximate the rules of the real physical world as much as possible.

Lua, Times's first choice, is a virtual machine with optimized compiler and bytecode. Suitable for the blockchain application, Lua enables static compilation and on-demand execution.

In blockchain networks, there are 5 stages of life cycle of smart contract.

(1)   Create source code in Lua.

(2)   Compile to GPC bytecode.

(3)   Contract registration & Contract account deposit.

(4)   Call contract API.

(5)   Upgrade or destroy the contract.

For economic consideration, tokens will be spent only when registrations, calls and upgrades occur. On the one hand, the execution of contracts must take up computer resources, blockchain capacity, and network traffic. On the other hand, economic means raises the threshold of potential cyber-attack.

The separated module for contract execution, Lua virtual machine (LVM), functions as follow:
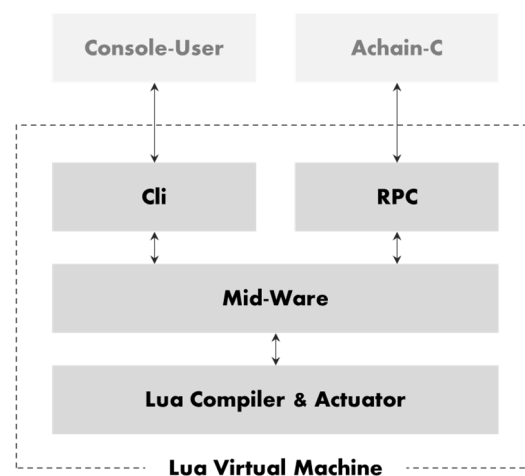
Architecture of LVM

The LVM includes 4 parts, they are CLI (Command Line Interface, RPC (Remote Procedure Call, Mid-ware and LCA (Lua Compiler & Actuator.

How LVM works? Firstly, contracts are entered from the console as form of Lua command line. Second, the CLI receives command and transfers it to the Mid-ware. If the RPC receives Lua request from blockchain at the same time, the Mid-ware will transfer both command and request to LCA synchronously. At the end, LCA runs the execution environment, receives Lua script, and executes program and feedback results to the Mid-Ware. The CLI and the RPC return the results from Mid-ware to the console and the blockchain separately.

There's a frequent demand to execute contract within an active blockchain network. To ensure high efficiency, Times follows two principles. First is minimizing the startup and shutdown time of the LVM process. Second is ensuring execution outputs to be consistent at different nodes and different time with identical inputs.

LVM supports more advanced program languages, such as C#, Java, Solidity (Ethereum program language. That enables most of developers and enthusiasts to get involved.

3.2 Consensus agreement

The blockchain network cannot work without consensus. At present, widely available consensus solutions are: PoW, PoS, PBFT and DPoS. Times selected the DPoS and improved it into a new mechanism named RDPoS (Resulted-Delegated Proof of Stake).

The RDPoS inherits all the advantages of DPoS. Not only is it unnecessary to consume redundant computing power to get a new block, but also are the execution results of contract able to be verified by agent node or all nodes alternatively, depending on the state of networks.

It's unable to establish the community consensus without incentive, which is usually called token in the blockchain world. Times is such a public blockchain with its own token, ACT. The ACT-holders have the right to involve in the community events, such as creating and publishing smart contracts, accessing network service, voting agents, getting profits as an agent. In Times community, candidates are voted by all of ACT-holders, the top 99 candidates with the highest number of votes will upgrade to agents and get the right to verify transactions in turn. No one can modify the verification sequence by itself. Work exchange rewards, no work would be punished.

Theoretically, RDPoS enhances the network transaction capability better than DPoS. Specially in that case of long-time execution or high-usage of storage, all nodes, not just the agent node, take part in verification. The RDPoS can reduce the congestion level of whole networks. Moreover, by optimizing consensus mechanism, the members in group of agents always change. This is important for the networks to keep decentralized.

3.3 Account

Account is specially designed for secure transactions during the blockchain networks. There are 3 elements need to be mentioned when we talk about blockchain theory, account, public key and private key: private key – public key – account, in a specified order. Thanks to the SHA (Secure Hash Algorithm) method, blockchain is a secure network because private key is too hard to be cracked reversely. The hash value is a refinement of an object, something like software, email, webpage etc. Usually its output has fixed capacity and is smaller than the input. Detailed generation process is as follow.
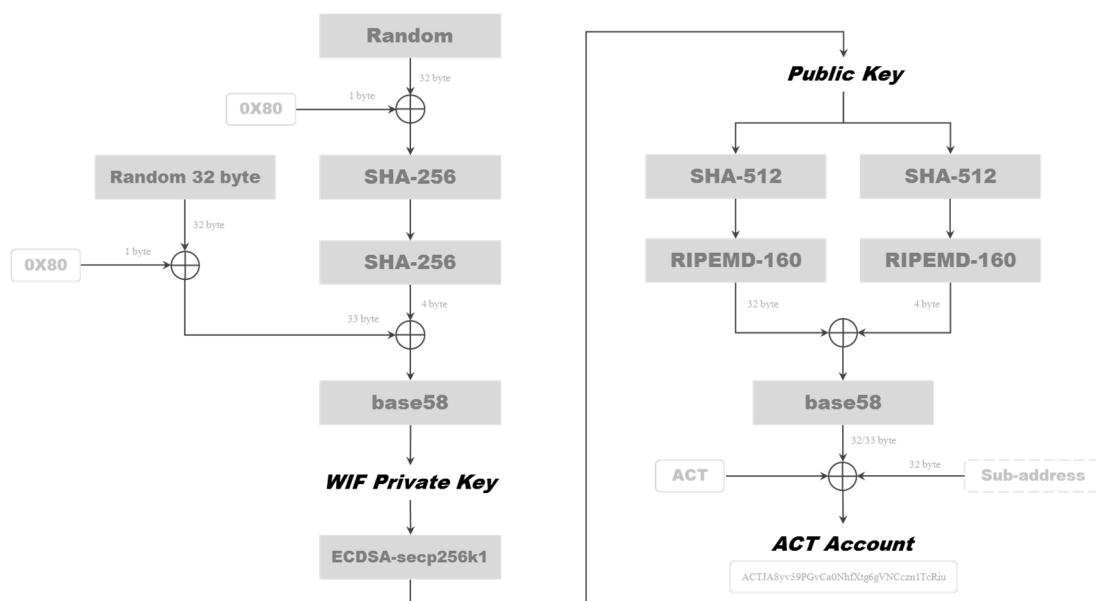
Generation process of private key, public key and ACT account

We divide accounts into two kinds according to the byte length, the main account and the sub-account.

The main account contains 35 or 36 bytes but sub-account 67 or 68 bytes. Obviously, the sub-account has more bytes than the main one, because the sub-account contains a main account and another 32-byte random characters. For this reason, main account can associate with lots of sub-accounts, as long as all of them have the same first 32 or 33 bytes. It's easier to improve transaction performance with help of such design. Parallel transactions among different sub-accounts are allowed if those sub-accounts belong to a main one. The main-sub design is mainly used in cryptocurrency exchange for saving account consumption.

Times selected the account model instead of UTXO (Unspent Transaction Output) model, which is applied to Bitcoin. UTXO is an excellent design with features parallel transactions and better anonymity. It is, however, very difficult to realize smart contract under transaction-oriented design. It's easier to initiate transactions through triggers caused by state or conditions changes.

3.4 Forking network

"Hard Fork Will Make Network More Resilient," asserted the Ethereum Foundation Co-Founder, Taylor Gerring.

Times advocates for proper fork network for two reasons: First, hard forking keeps the network vigorous; Second, hard fork satisfies different application scenarios. Blockchain network is a kind of social consensus supported by people in the community. When social consensuses change, hard forking will be inevitable. Some forking blockchain will survive and others die due to lack of support. Forking signifies the process of evolution of any distributed autonomous organization, and eventually each survived forking blockchain prove to better solve real-world problems. Secondly, blockchain is still in early stage of development. Besides cryptocurrency, other use cases based on blockchain still need be verified. Many technologies, such as lighting network, zero knowledge proof, side chain, and segregated network, emerged recently in blockchain field. These innovations demonstrate that different transaction rate, different consensus algorithm, and different technology characteristic could be combined together to satisfy different requirements. Ideally different forking network will meet corresponding needs. Although, forked network may also generate new issues, which will be discussed in the next section.

Times is designated as the initial blockchain. From Times, user can fork multiple new blockchains easily, and user can even fork from newly created blockchain continuously. All forked blockchains are equal, which means they are not hierarchical from technical or economic perspective. VEP (Value Exchange Protocol will record and broadcast the message about newly forked blockchain, which includes genesis block, blockchain identification, seed nodes, cryptocurrency, service identification etc. Each forking will trigger a new VEP message broadcasting. When blockchain need to communicate with each other, the node in the blockchain will find nodes in another blockchain from VEP broadcasting message, and exchange information and values under VEP infrastructure. VEP works like DNS service, which provides with registration, update, and access services.

In order to achieve these goals, Times sets up its BAAS (Blockchain as a Service), and utilizes multiple programming languages and visualized development to reduce the difficulty of adoption. Anybody could utilize forking network to develop his own application, so as to encourage community innovation. When the Times community becomes more active, Times value will increase, more and more developers will join Times forking network. This mutual stimulation will prosper Times ecosystem.

3.5 Value Exchange Protocol

VEP is a cross-chain communication protocol. A single blockchain has its limitation to support so many different applications, but a connected blockchain network could produce overlaid value. The more forking blockchains are connected, the more values are created. Before we discuss how VEP works, let's see how nodes trust each other within a blockchain network. Blockchain stores unchangeable and trustable information, which relies on distributed ledger and distributed

consensus algorithm. Blockchain is also a community based on agreed consensus, nodes in blockchain trust each other based on such consensus and economic inspiration. In the same way, the whole blockchain could be taken as a "node", and when numerous "nodes" connected, "nodes" need a new consensus among the forking blockchain network. It becomes more difficulty because the forking blockchain network need also equality, trust, and balance different interest, not to mention evil nodes in the network. So it is important to setup rules in advance, just like human need cooperate across organizations under certain laws, contracts, and morals.

VEP defines the rules of connection and communication. VEP registers each forking blockchain, and provides query and access service for each licensed forking blockchain. VEP supports two major user scenarios: cross-chain communication and cross-chain smart contract invocation. Cross-chain communication means that smart contracts communicate and invoke with each other, with possible new data creation, which are triggered indirectly by ledger or offline data changes. For instance, overdue loans, which are defined in smart contract, will impact personal credit. The loan records are stored in blockchain A, credit information is stored in blockchain B, and personal identification is stored in offline public database. A simple example about cross-chain smart contract invocation is cross-chain token exchange, which guarantees an unchanged total value.
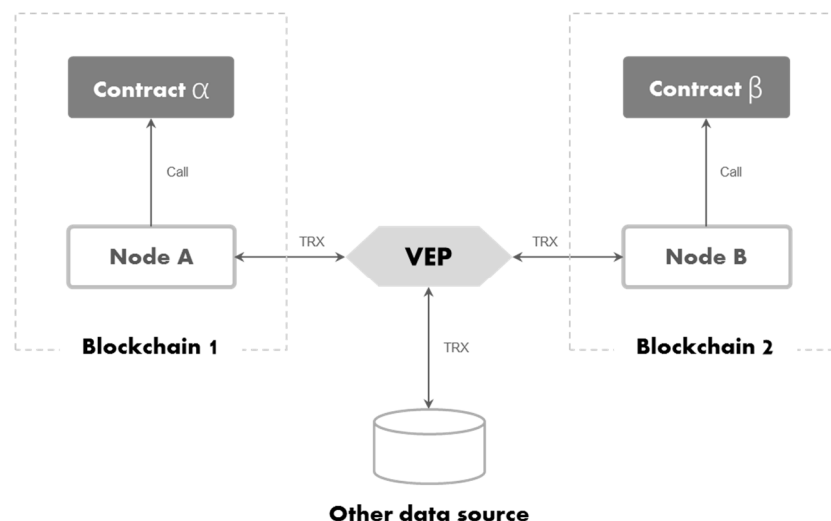
Cross-chain communication
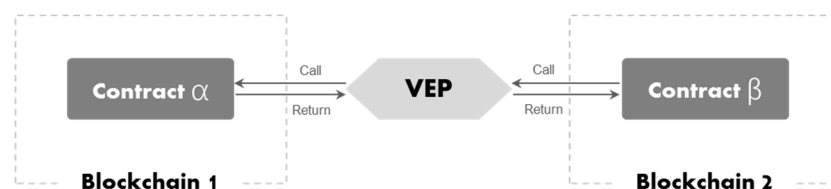
Cross-chain smart contract invocation

VEP includes following information:

(1)   Blockchain registration information, network identity, service identity, seed nodes, etc.

(2)   Cross-chain verification protocol.

(3)   Communication protocol.

(4)   Assets exchange protocol.

(5)   Rewards and punishments mechanism.

3.6 Event-driven

Based on VEP, forking Times network can communicate and exchange values. Through IOT (Internet of Things) and AI (Artificial Intelligence), forking Times network can even embrace offline data, such as enterprise and public database, into Times network, and finally achieve real time event driven from real world.

There are 5 steps for event-driven mechanism:

(1) Recognize different scenes, categorize them, and setup response standard.
(2) Open listening service and catch information.
(3) Calculate and check response.
(4) Execute smart contract through VEP.
(5) Return execute result.

4 Applications

4.1 Supply Chain Finance

Supply chain finance, also known as supplier finance or reverse factoring, is a set of solutions that optimizes cash flow. It enables businesses to extend their payment terms to their suppliers while allowing their large and SME suppliers to get paid early. It is one of the fastest growing industries in recent year. However, there is too many parties involved, which leads to scattered data storage. Supplier's inventory information is listed in its warehouse management system; the deliverable information is located in the CRM of logistic company; the funding information is allocated in the bank; and the operation data is in the hands of the enterprise itself. It is very difficult to build a credit system since all the data is non-transparent and incomplete. Therefore, the financial institutions will to be very cautious and miss some good projects eventually due to huge cost of credit assessment.

Times can help enterprises and financial institutions rebuild a credit system to optimize efficiency of supply chain finance. The solution is to build an Times-based enterprise credit system that involves warehousing, logistics and financing services providers. The blockchain-based system enables all the companies in the supply chain to access all the data collected during production, logistics and auditing. E-receipt will be utilized and its issuance, confirmation, circulation, splitting and acceptance are triggered through smart contracts by various parties in the supply chain. And it will only be triggered and recorded when data was updated in one of the enterprise's system, which was mutually agreed between all parties. All actions made in the system will be recorded and stored in the blockchain and cannot be modified or deleted.

Times leverages technologies such as BaaS and smart sandbox to enable fast-track deployment on the blockchain. It allows the users to quickly build a blockchain network by folk at a low cost. In addition to that, Times accepts using of VEP to establish a connection protocol and activates the event-driven mechanism by integration of data. In this case, all participants are able to verify the data to ensure the transfer of funds in the supply chain with improved efficiency.

4.2 Authentication

The retail industry is naturally characterized by the fragmentation of transaction data, the diversification of trading nodes and the complexity of trading networks. The packaging of an item usually labels its date of production, place of origin and manufacturer regardless of its sales channels. However, it is difficult to verify the listed information. Huge profit margins create great incentives for fraud, especially for high-value goods, such as diamonds, luxury bags and skin care products etc.

The existence of fraud harms consumer's interest and causes damages to the credibility and brand image of the authentic business. There are three major industry pains for authentication of goods. First, it has to trace back not only to its production process but also its logistic process – which involves high complexity in cross-organization cooperation. Secondly, the information is

isolated in different centralized systems used by hundreds of parties. Lastly, centralized system can be risky as the information can be changed or deleted by individual party.

Times proposed the solution to the retail industry – Blockchain + IoT

With IoT, data in production and logistics can be collected in real time through smart devices and be stored in Achain's traceable network through VEP. Blockchain's unique data storage structure and distributed ledger technology ensure that the data on the chain cannot be deleted or altered. Meanwhile, asymmetric encryption and anonymous mechanism ensure that information security. Customers can easily access the full profile of a product by providing its product code and batch number.

Blockchain can solve the pain of authentication while preventing disclosure of corporate information. The information is transparent to all relevant parties: manufacturers, logistics providers and the consumers. The purchase information and logistic details provide insightful support to the manufacturer for analyzing their production strategies. Such mechanism also benefits the logistic provider by giving data support. The blockchain technology makes a transparent and efficient society.

5 Development plan

5.1 Plan

Stage1. Singularity（2014~2016）

The first stage is to enhance the Times network's security and stability. Smart contracts, digital assets, and sandbox simulations are made available through the methodology of modular design. Sandbox can automatically test and monitor the environment where the newly created smart contracts operate. Thereby they ensure that those contracts run stable and safely within the Times network.

Stage2. Galaxy （2016~2017）

Times splits into multiple sub-chains to meet the need for different applications in the reality, including insurance, e-documentation, cryptocurrency, record investigation, credit rating, and much more can be fulfilled by sub-chains within an interconnected, low-cost, user-friendly, and customized blockchain network.

Stage3. Cosmos（2017~2018）

Stage3. The BaaS and VEP (Value Exchange Protocol concept and technology can not only unify the main chain and sub-chains but also connect the non-blockchain realities to the blockchain ecosystem. This pushes the world's interconnections to a greater, all-encompassing dimension.


Times Development Plan

6 Program governance

6.1 About Times Foundation

The Times Foundation is responsible for Achain's development, its transparency in administration, and communications within its community network. The Foundation creates an efficient and sustainable administration structure to facilitate with the community's affairs management. It also secures funds that Times receives. It is consisted of a strategy center, a technological development center, a marketing center, and an administration center.

6.2 Foundation governance

| Eco-Strategy | Development | Marketing & Operation | General Administration |
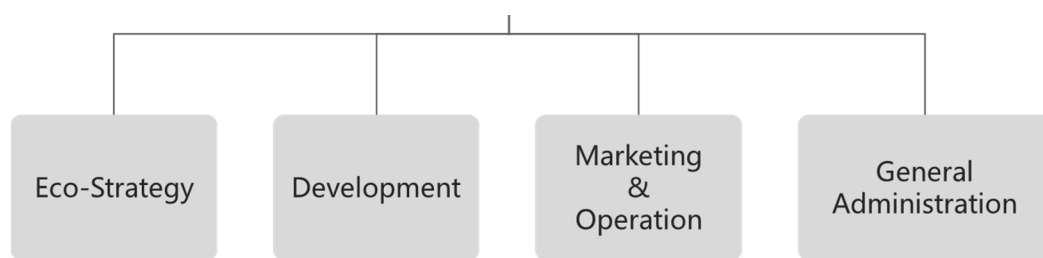
Foundation Governance Structure

Below is a detailed introduction to all sectors:

The Strategy Committee is responsible for managing and decision-making of all major events. This might include hiring or dismissing executive personnel, and much more. The membership of the Strategy Committee lasts for 3 years with extendable terms of service. The Committee Chair is elected by the Times founders and shareholders in the first term and by all members of the Committee in the following terms.

The Eco-Strategy Center is responsible for Achain's cross-industry cooperation, especially focusing on forming into strategic partnerships with companies from the fields of Internet financing, ICO, cross-border trading, the Big Data, and AI. This prepares Times for wider commercial uses.

The Development Center is responsible for advancing, testing, announcing, and inspecting basic technologies. Members of the center maintain a healthy communication with benefiters and contributors regarding progress of projects. This might involve holding regular technology conferences and meetups.

The Marketing & Operation Center is responsible for promotion and communication of new technologies, products, communities, and projects.

The General Administration Center serves for finance, legal affairs, human resources, and

other administrative functions. Finance involves planning, exercising, and reviewing budgets for all projects. Legal affairs involve composing and reviewing documents of all types to eliminate any risks of illegitimate practices. General administration is responsible for human affairs such as appointment of positions and distribution of salaries.

6.3 Contact us

Official website: https://charterhouse-inv.com/

6.4 Open source

Github: https://github.com/TimesChain/Times

7 Technical Team

Founded in 2015, Times owns a technical team of 6 core members who are fully experienced in blockchain and cryptocurrency technology.

Founder
CLARKE, Alan

Core Developers					
Rebecca Ja	Pierre De Jon	Riley Eiley	Niamh Cole	Amy Lambert	Joseph Holmes