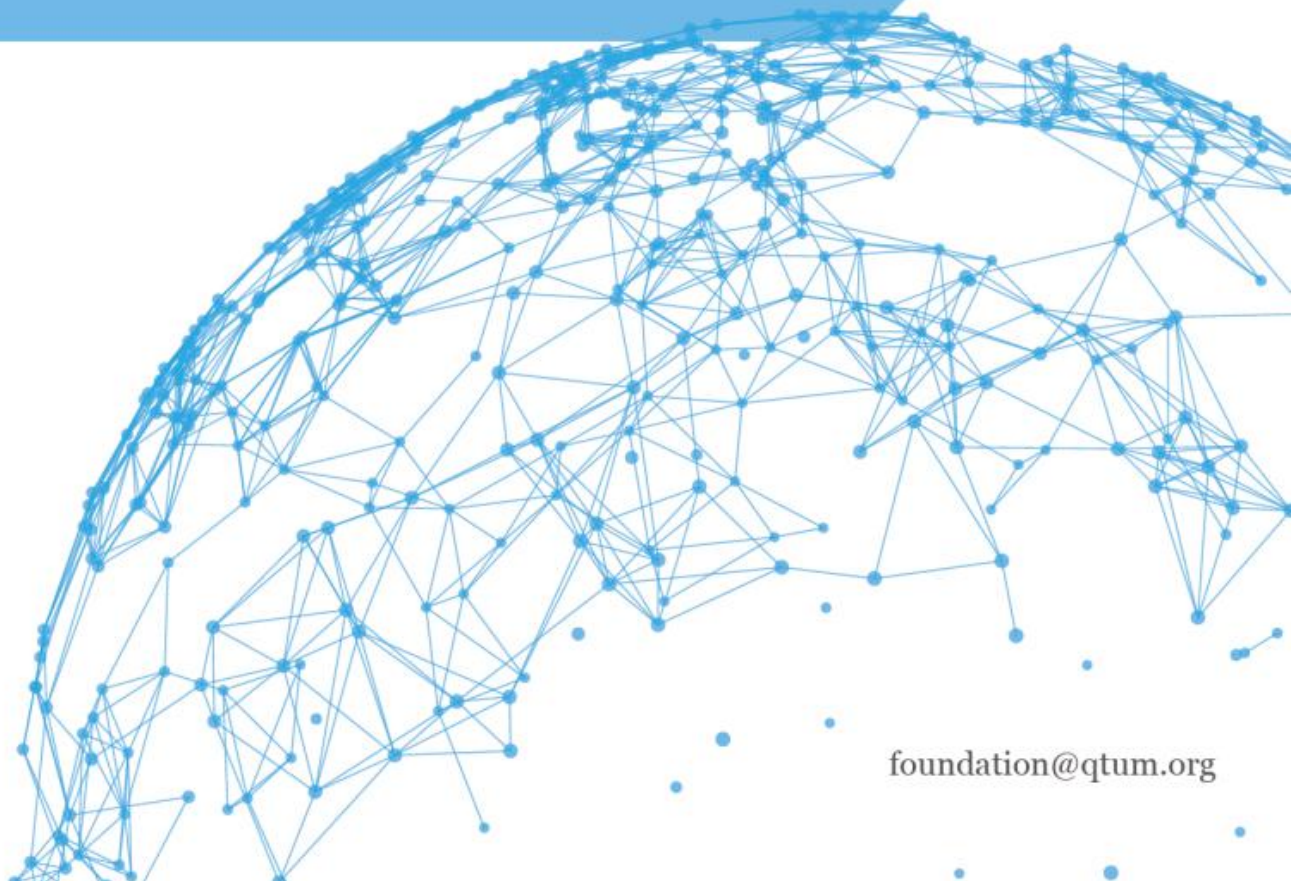




# QTUM BLOCKCHAIN ECONOMY WHITEPAPER

---

Qtum Foundation (Draft)



[foundation@qtum.org](mailto:foundation@qtum.org)





---

## Content

Abstract.....	4
1. Design Concept of the Qtum Blockchain.....	5
1.1 The Background and Significance of Blockchain.....	5
1.2 Why Do We Design the Qtum Blockchain.....	5
1.3 The Qtum Blockchain Design Principles.....	6
1.4 Vision of the Qtum Blockchain.....	6
2. Technical Characteristics of the Qtum Blockchain.....	8
2.1 Introduction to the Qtum Blockchain.....	8
2.2 Technical Model of the Qtum Blockchain.....	8
3. Governance Structure of the Qtum Blockchain.....	11
3.1 Establishment of the Foundation.....	11
3.2 Governance Structure of the Foundation.....	11
3.3 The Qtum Team.....	15
3.4 Human Resource Management of the Foundation.....	16
3.5 Risk Assessment and Decision-making Mechanisms of the Foundation.....	17
3.6 Daily Operation Mechanisms of the Foundation.....	18
3.7 Financial Management of the Foundation.....	20
3.8 Other Matters and Legal Affairs.....	24
4. The Implementation and Iterations of Qtum.....	25
4.1 The Qtum Blockchain Implementation Timetable.....	25
4.2 The Qtum Blockchain Crowdsale Plan.....	26
4.3 Future Iteration Plan of the Qtum Blockchain.....	26
5. The Qtum Blockchain Applications.....	27
5.1 Decentralized Applications (DApp) .....	27
5.2 Industry Oriented.....	27
5.3 Go Mobile Strategy.....	27
6. Business Use Cases.....	28
Appendix 1 Glossary.....	31
References.....	32
Revision History .....	33



---

## Abstract

The Qtum Blockchain (“Qtum”) is committed to develop an open source ecosystem for the blockchain community different from that of Bitcoin and Ethereum. It utilizes a Value Transfer Protocol (“VTP”) to achieve the transferring of value from peer to peer and to build up a decentralized application platform, which brings blockchain technology into the financial services, Internet of Things (“IoT”), supply chain management, social media, gaming and other industries. Innovative technology, comprehensive governance structure and board applications give Qtum advantages over Bitcoin and Ethereum as a public blockchain.

- **From a technical point of view**, the highly qualified Qtum development team brings in the technology of identity, Oracle and Data feeds, and is committed to achieve the first IPoS (“Incentive Proof-of-Stake”) Smart Contract platform, which is compatible with Bitcoin Improvement Proposals (BIPs based on UTXO model). In terms of compliance, Qtum meets the regulatory requirements from different industries.
- **In terms of governance**, Qtum established the Qtum Blockchain Foundation (“Foundation”), which is committed to develop the Qtum Blockchain, to advocate governance transparency, and to promote safety and harmony of the open source ecosystem. In order to ensure the sustainability, management effectiveness, and fund-raising security of the project in the open source community, the Foundation uses a governance model that considers the various dimensions of the project, including code management, financial management, public relations management, and other dimensions to operate and to deal with general affairs and privileged operations.
- **Regarding the applications built on Qtum**, they bring in the off-chain factors that are used in Decentralized Applications (“DApp”) and Smart Contracts to connect the real world business logic with the blockchain world. By supporting multiple industries and methods, the applications will follow the Go Mobile strategy. In Qtum’s open environment, we not only support and promote the Go Mobile strategy, but also provide mobile services with third party developers, including mobile wallets, mobile DApp store, mobile smart contract applications, etc. In addition, we encourage third party developers to join us and help develop mobile blockchain services for Internet users.

The Qtum Blockchain, as the most promising Blockchain ecosystem, perfectly combines the advantages of Bitcoin and Ethereum and addresses the inherent problems of existing blockchain systems. It will continue to develop and iterate through the foundation of the platform, as well as through the products and practical business implementations. A new kind of economy mode will be formed by the Blockchain Economy to significantly enhance the efficiency of the industries, as well as society as a whole.

Qtum, defining the Blockchain Economy.

©Qtum Foundation. All rights reserved.



# 1. Design Concept of the Qtum Blockchain

## 1.1 The Background and Significance of Blockchain

Before the emergence of the Bitcoin network, the TCP/IP protocol has been widely used to transmit information globally. The development of interconnection technology (e.g., Internet, Internet of Things, and Virtual Reality/Augmented Reality) have introduced more diverse ways to interact among people, information and objects and allowed more entities to become digitalized and tokenized. However, information sharing and transmission is not enough to meet the development needs of the economic society. A question has been increasingly raised and discussed by the public: How can we transfer digital assets and value from peer to peer?

On the 31<sup>st</sup> of October 2008, Satoshi Nakamoto announced the Bitcoin whitepaper titled “Bitcoin, A Peer to Peer Electronic Cash System” and introduced the Bitcoin network to establish a decentralized system of value transfer. Every participant in the Bitcoin network acts as a reviewer of transactions; the value transferred between two parties can be completed without establishing a trust relationship. This technology has changed the way we obtain and share value and has created a new decentralized, peer-to-peer community.

In the past, we were not able to identify a solution to transfer assets and value from peer-to-peer over the Internet without the involvement of third parties. The Bitcoin network is the first P2P Value Transfer Protocol (“VTP”). In this Qtum Blockchain whitepaper we introduce the practical implementation of a VTP over the Internet.

At present, with the development of blockchain technology, implementing blockchain applications are not limited to Bitcoin or Ethereum. In the Qtum blockchain, we integrate on-chain and off-chain data to form a third blockchain community, which further achieves peer-to-peer value transfer by utilizing Qtum’s VTP.

## 1.2 Why Do We Design the Qtum Blockchain

Since Bitcoin published its source code in 2009, multiple altcoins and other blockchain projects appeared in the community, including Ethereum, which aims to become a universal platform for Smart Contracts and Decentralized Applications. However, the blockchain industry still faces many technical and implementation challenges. The main issues are as follows:

1. Lack of a new and more capable Smart Contract platform. The lack of interactions with real world data has resulted in the limitations of implementing Bitcoin and Ethereum into industries;
2. Compatibility of different blockchain technologies. For example, Bitcoin is based on the UTXO model, which is not compatible with the Ethereum’s Account model;
3. Inflexible consensus mechanism. Different participants in the public blockchains and consortium blockchains require different types of consensus mechanism;



4. Lack of industry compliance considerations. For example, existing blockchain systems are not able to fully meet the regulatory requirements such as the Anti-Money Laundering (“AML”) and Know-Your-Customer (“KYC”) in the financial industry;
5. Current blockchain systems operate as closed systems. At present, most of the Smart Contracts are triggered by the blockchain system itself, lacking an interaction with the real world.

We hope to build an entirely new blockchain ecosystem, Qtum, as an alternative option for VTP in the world and to move the ease of use of the entire blockchain industry one step forward.

Qtum is based on the UTXO model and uses the Ethereum Virtual Machine (EVM) to achieve the compatibility between Bitcoin and Ethereum for public blockchain. It utilizes Oracle and Data Feeds, in conjunction with the logic of regulation, to bridge the real world to the blockchain world.

### **1.3 The Qtum Blockchain Design Principles**

The design principles of Qtum are mainly to solve the limitations and practical implementation problems of blockchain technology. The principles are listed below:

1. Create an entirely new kind of smart contract called Master Contract that can execute a contact triggered by off-chain and on-chain factors;
2. Achieve compatibility with different blockchain technologies;
3. Allow industry focused consensus mechanisms for public blockchain;
4. Take regulations into consideration and provide an Identity module;
5. Interact with the real world by executing Master Contracts triggered by off-chain inputs.

Moreover, the Qtum blockchain provides a modular design and usability concept. For the convenience of development and maintenance, Qtum is divided into three modules: Qtum Tech, Qtum UI and Qtum Business.

At last, we provide different versions of the Qtum system – even mobile services for all operating systems and development requirements. We highly encourage third party developers to work with us to facilitate the implementation of blockchain technology that will benefit more Internet users.

### **1.4 Vision of the Qtum Blockchain**

Qtum is committed to create a globally influential open source community by cooperating with other blockchain communities, third-party developers, and technical innovations. The ultimate goal of Qtum is to bring blockchain technology into the finance, social media, gaming, Internet of Things (“IoT”), and other industries. Qtum is a compatible ecosystem;



it utilizes Oracle and Data Feeds, in conjunction with the logic of regulation, to bridge the real world to the blockchain world.

**Technical innovation:** As an open source community, the Qtum Blockchain has built a platform that is secure, reliable, and compatible with the Ethereum community and the Bitcoin system. It also integrates on-chain and off-chain data through technical and conceptual innovation.

**Sustainable development:** In order to realize the sustainable development of the Qtum Blockchain and to avoid the layered structure and differentiation of the underlying structure, the Qtum Foundation will govern the community by following the established rules and principles, including the management of general affairs, code, financial, compensation, scope of privileged operations, etc.

**Business application:** The Qtum Foundation will reference investment banking practices to perform industry analysis and selections and to choose the appropriate industries to implement Qtum technology. Enterprises on the Qtum blockchain will be able to develop more applications in order to achieve the sustainable development of Qtum.

**Business partners:** Through collaboration with business partners and integration of resources from companies, businesses, technology communities and governments, the Qtum Foundation will make the most efficient use of shared resources to achieve synergetic development with society.

The foundation will provide transparency for financial management, code management and business practices, and will maintain high standards of honesty, ethical business conduct and compliance with applicable laws, rules, and regulations. An accounting firm has been engaged to provide financial report audit and compliance management services.

To further make the Qtum Blockchain a truly open source community, the Qtum Foundation will eventually distribute 80% of the total Qtum tokens to the community for business implementations, marketing promotions and linkages between the real world and blockchain world. The remaining 20% tokens will be allocated to the co-founder team, early backers, consultants, and development team.

The birth and the infancy stage of Qtum have been strongly supported by the founding members, the development team, industry experts, early backers, lawyers and professional consultants. We would like to thank the following people (partial list below) who have made extraordinary contributions to the development of the Qtum Blockchain Economy.

Patrick Dai (Co-founder)	Neil Mahi (Co-founder)	Jordan Earls (Co-founder)
Anthony Di Iorio (Backer)	Weixing Chen (Backer)	Jeremy Gardner (Backer)
David Lee (Backer)	Bo Shen (Backer)	Xu Star (Backer)
Xiaolai Li (Backer)	Jehan Chu (Backer)	Ming Sun (Legal Advisor)

## 2. Technical Characteristics of the Qtum Blockchain

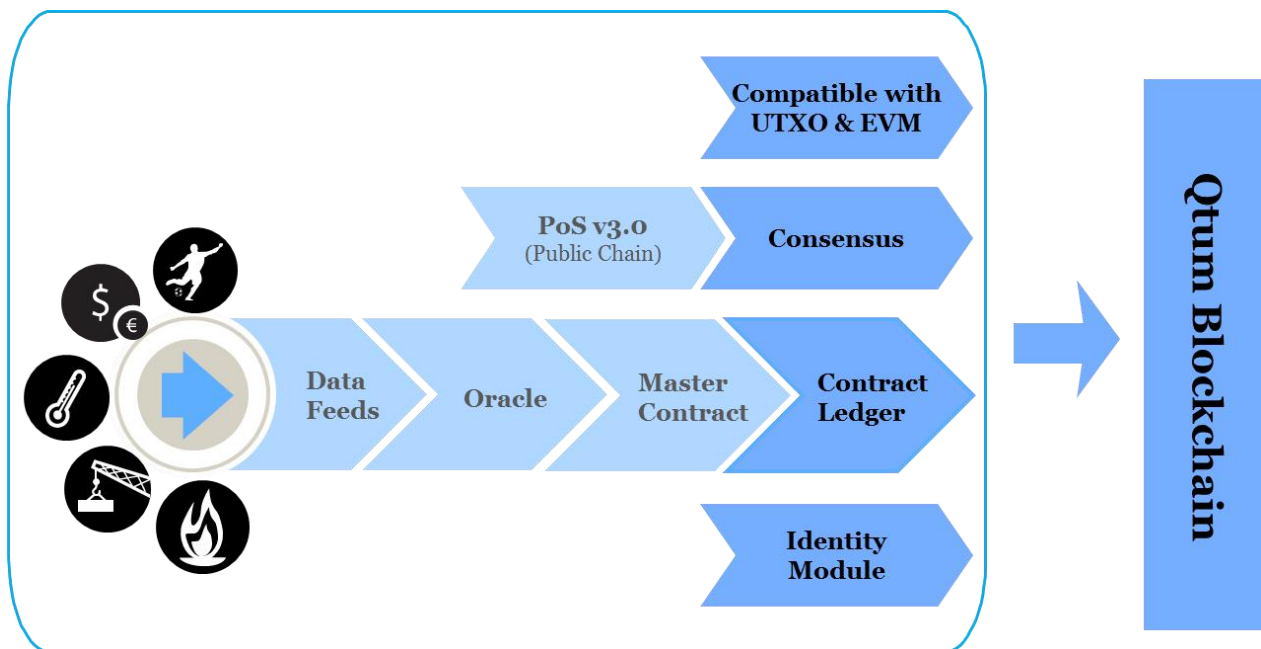
### 2.1 Introduction to the Qtum Blockchain

Qtum is committed to develop an open source blockchain community that is compatible with that of Bitcoin and Ethereum. Qtum’s development is industry-implementation-oriented; it brings the advantages of blockchain technology to all users from various industries by developing decentralized mobile applications.

Qtum pays more attention to the practical applications of smart contracts. It introduces Oracle, Data feeds and an Identity Module from third parties to fulfill the compliance requirements from traditional Internet enterprises, including finance, IoT, etc.

In addition, Qtum focuses on decentralized application development. Together with third party developers, Qtum aims to build the ecosystem community and to provide a great number of decentralized applications for all users.

### 2.2 Technical Model of the Qtum Blockchain



- **Compatible with UTXO & EVM**

The Qtum blockchain uses the UTXO model to ensure the consistency of transactions and the traceability of tokens. In addition, all smart contracts developed for Ethereum are able to operate on the Qtum blockchain with minimal changes, if any. Qtum’s blockchain perfectly combines the advantages of both Bitcoin and Ethereum networks and addresses the inherent problems.





- **Consensus**

Proof-of-Stake consensus mechanisms are used for the public blockchain. In the later phase of development, we plan to introduce the concept titled “Incentive Proof-of-Stake” (“IPoS”), which will bring in incentive reward mechanisms that take the estimation of online nodes into consideration.

- **Contract Ledger**

In the Qtum blockchain, the Contract Ledger stores all smart contract content in a readable format. It allows users to download the code and contracts in a peer-to-peer network based on their own interests. The Contract Ledger provides greater transparency, readability, and audibility.

Data feeds are the data resources obtained from off-chain. The Oracle selects the most suitable data to trigger the execution of smart contracts, which are stored in a readable format in Qtum. In the Qtum blockchain, we introduce the role of regulators to avoid major incidents, such as the DAO.

- ✓ Data feeds

Data feeds represent the data obtained from off-chain sources (such as currency exchange rate, GDP, the temperature of a city, competition results, etc.), which are input into the blockchain to execute smart contracts or decentralized applications.

For example, if the room temperature were to drop to 10 degrees Celsius, the air-conditioner would switch to “heating mode”. In this case, the temperature data from thermometer can be considered as a data feed, which is obtained from off-chain (i.e., real world).

- ✓ Oracle

In the Qtum blockchain, the oracle could represent a specific trusted organization, an entity, a node, or a public key address. When there are multiple data resources for an inquired data input, the oracle selects the most suitable data resource based on a pre-defined rule.

- ✓ Master Contract

In the Ethereum network, only data obtained on the blockchain can be used as a trigger to execute the smart contract. However, one of the most remarkable innovations of Qtum is that off-chain factors can also be the trigger. For such contracts, we will refer to them as Master Contracts.

- **Identity Module**

As we know, financial institutions usually have more requirements regarding identity authentication and data security. With the introduction of third-party credit bureaus,



---

users in the Qtum network that have been authenticated by the Identity Module will be granted higher priority.

For details on the technical characteristics and implementation model please refer to the “Technical White Paper.”



---

## **3. Governance Structure of the Qtum Blockchain**

### **3.1 Establishment of the Foundation**

The Qtum Blockchain Foundation (“Foundation”) is a non-profit organization established in Singapore in November 2016. The Foundation is committed to develop the Qtum Blockchain, to advocate governance transparency, and to promote safety and harmony of the open source community.

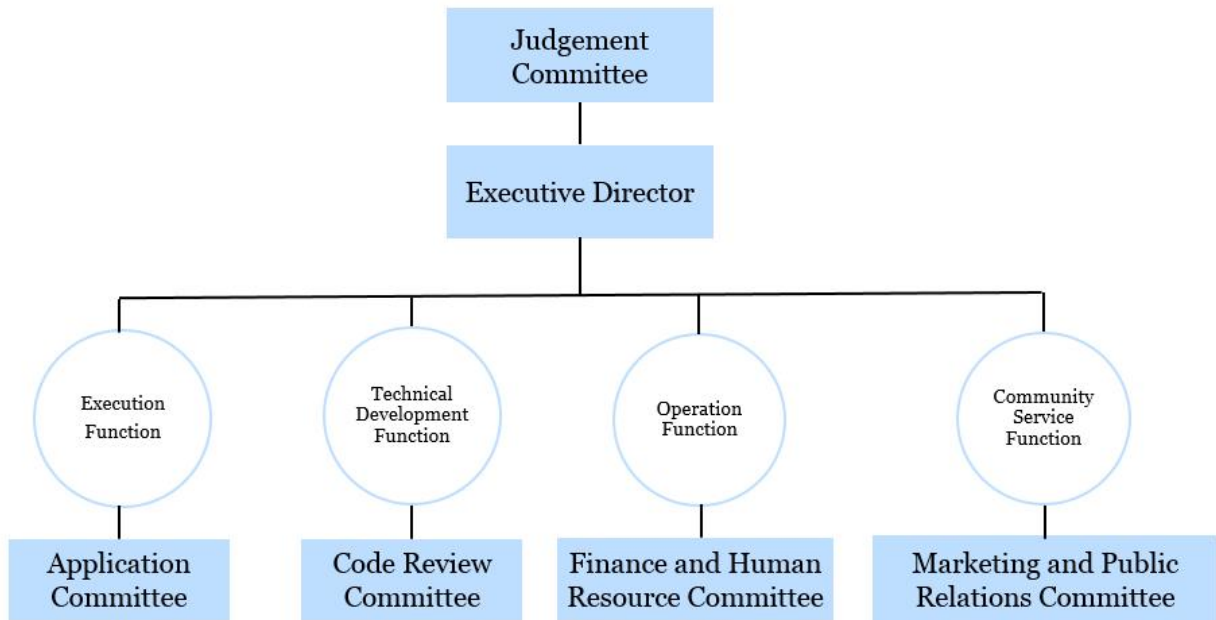
The attempt to implement a hard-fork to restore the stolen Decentralized Autonomous Organization (“DAO”) tokens have created doubts in Ethereum and the concept of decentralization of blockchains. In order to avoid the inconsistency of transactions on the client side or other occurrences that are contrary to the design concept of blockchains, the Foundation is committed to develop a robust governance structure and to provide managerial assistance to general affairs and other privileged matters.

The design of the Foundation’s governance structure mainly considers sustainability, management effectiveness, and fund-raising security of the projects in the open source community. The Foundation consists of developers and functional committees. The organizational structure is made up of the Judgement Committee, the Code Review Committee, the Finance and Human Resource Committee and Marketing and Public Relations Committee. In the early stage of the Foundation, members of the Judgement Committee are Chairman Patrick Dai, the core developers and private backers. The term duration of committee members is set at two years.

### **3.2 Governance Structure of the Foundation**

A governance model is established to manage the daily operations and special occasions with detailed operational procedures and rules. The section will depict the governance structure and the roles and responsibilities of each function. (See below)

## Qtum Blockchain Foundation



- **Judgement Committee**

The Judgement Committee is responsible for appointing or dismissing the executive director and leaders of each functional committee, making important decisions, holding emergency meetings, etc. The term as judgement committee chairman and other members is two years; the chairman shall not be eligible for re-election.

The members of the first Judgement Committee have extensive experience in the blockchain industry. A brief introduction of the committee members is listed below:

Name	Experience
Patrick Dai	Patrick is the founder of the Foundation. He graduated from the Draper University, and Chinese Academy of Sciences. Previously employed by Alibaba, and committed to the blockchain technology development and research for a Doctorate Degree, with abundant blockchain industry development experience.
Neil Mahi	Neil has 20 years' experience developing software and has four years' experience in the blockchain space. Neil has a Master's degree in Business Administration from ISCAE, but later specialized in computer science. Neil was also a professional poker player and speaks four languages.



Name	Experience
Jordan Earls	Jordan is a trusted and well-known member of the cryptocurrency community and has been developing software since he was thirteen. Jordan has reviewed over 100 altcoins and identified multiple exploits in coins.
Bo Shen	Mr. Shen is the founding partner of FenBuShi Capital which is the first venture capital firm that exclusively invests in Blockchain-enabled companies.
Ming Sun	Mr. Sun provides professional legal consultancy services in mergers and acquisitions, banking and trust, digital currency and distributed ledger technology.
David Lee	David is a co-founder of LeftCoast at Silicon Valley, he is specializing in distributed ledgers technology, big data, and machine learning.
James Gong	James is a famous writer in the blockchain community, and is committed to promote the development of blockchain and distributed ledger technology.
Jason Fang	Jason is an associate at FenBuShi Capital, he was previously working as the director of marketing and operations at Wanxiang blockchain labs.
DJ Qian	DJ is the co-founder of BitSE, which is an innovative company focusing on blockchain application development.

After the first term, the community will elect 50 representatives based on the number of Qtum tokens and weighting, 9 of which will then be elected as core members of the Judgement Committee to make important and emergency decisions. The Judgement Committee members shall be subjected to credit investigation and public emoluments during their tenure.

The following matters are subjected to the Judgement Committee to vote via registered ballot. Each member has one vote and the Foundation chairman has two votes. The decisions of the Judgement Committee shall be made based on the votes of the majority (more than half):

- ✓ Changes to the governance structure of the Foundation;
- ✓ Appointment or dismissal the executive director and leaders of each functional committee;
- ✓ Important decisions;
- ✓ Appointment and resignation of the Judgement Committee members during their term of office, such as violation of laws, administrative regulations, active abdication, etc.;
- ✓ Emergency events (e.g., the events affecting the entire community, system security breach, etc.)



In addition, when one of the following circumstances occur, the Executive Director shall convene the Judgement Committee members and hold an interim meeting within 5 business days:

- ✓ When the chairman deems it necessary;
- ✓ When more than one third of the Judgement Committee members make a joint proposal;
- ✓ When the executive director makes a proposal;

The meetings shall be attended by the Judgement Committee members. Those who cannot attend the meetings are allowed to delegate other members to vote, but are otherwise deemed to abstain from voting.

- **Executive Director**

The executive director shall be elected by the Judgement Committee. The position is responsible for daily operations, coordination with subordinate committees, presiding the Judgement Committee meetings, and other matters. The executive director shall report to the Judgement Committee on a regular basis.

- **Application Committee**

When the underlying infrastructure is fully developed, the Qtum Application Committee will select suitable industries to implement the Qtum blockchain in the real business cases.

- **Code Review Committee**

The Code Review Committee is made up of core developers in the Qtum development team who are responsible for the underlying technology development, API development, product development, etc. Developers shall hold weekly meetings to track project status and communicate progression and requests. Committee members follow the updates and hot topics from the community, maintain communication with the token holders inside the community and organize technical workshops occasionally.

- **Finance and Human Resource Committee**

The Finance and Human Resource Committee is responsible for the project financial monitoring, developer compensation, operation expenses monitoring, recruitment, talent management, performance review and staff on-boarding and off-boarding. The current daily accounting function is temporally outsourced to a third party.

- **Marketing and Public Relations Committee**

The Marketing and Public Relations Committee shall serve the community and promote Qtum technology, products, and open source projects. In addition, the committee shall make public announcements and respond to public affairs.



### 3.3 The Qtum Team

The members of the Qtum team are extremely experienced in the blockchain industry, as well as the within the cryptography and digital currency communities. The development team consists of 17 developers and is led by Patrick Dai. The development of the Qtum prototype has been completed. Main team members from the Qtum team are as follows:

Name	Experience
Patrick Dai	Graduated from the Draper University, and Chinese Academy of Sciences. Previously employed by Alibaba, and committed to the blockchain technology development and research for a Doctorate Degree, with abundant blockchain industry development experience.
Neil Mahi	Neil has 20 years' experience developing software and has four years' experience in the blockchain space. Neil has Master's degree in Business Administration from ISCAE, but later specialized in computer science. Neil was also a professional poker player and speaks four languages.
Jordan Earls	Jordan is a trusted and well-known member of the cryptocurrency community and has been developing software since he was thirteen. Jordan has reviewed over 100 altcoins and identified multiple exploits in coins.
Caspal OuYang	Caspal is an experienced web developer and has worked at Baidu. Caspal has more 21 gold medals for Rubik's cubing 1 record in Asia and 29 records in China. Caspal was ranked #1 for solving a 4×4 & 5×5 blindfolded and ranked #1 for solving a 3×3 Rubik's cube with his feet in China.
Baiqiang Dong	Baiqiang studied physics at Peking University and has worked for several software companies including Jinshan Software and Cheetah Mobile.
Mike Palencia	Mike is a blockchain technology developer and enthusiast, fell in love with blockchain since 2013 and has developed proof-of-concept platforms, block explorers, online wallets and one of the largest altcoin mining pools. Mike has taken part in several cryptocurrency projects since 2013.
Xiaolong Xu	Graduated from the Chinese Academy of Sciences. Previously employed by Microsoft and Tencent, Xiaolong has extensive experiences in software development and is passionate about blockchain technology development. He specializes in Linux development.



Time Markov	Time is C/C++/Qt/QML developer with 9+ years's experience in building cross-platform applications. With about one year experience in the blockchain space. Enjoy in working with this team.
Alexei Dulub	Alex is a full-stack developer experience in big data, blockchain technologies and security systems. Alex has worked on projects such as blockverify.io and OmniBazaar.
Brett Fincaryk	Brett worked as a Linux System's administrator from 1999 – 2004 and then worked at a Linux desktop support company from 2005-2014. His blockchain experience started in mid-2013, and met most of the Qtum's founding members in 2014.
Roman Asadchiy	Roman is a senior full-stack developer with over 3 years' experience building distributed blockchain solutions. Roman is in an expert in Bitcoin, Ethereum and smart contracts.
John Scianna	John has been following bitcoin since 2012 and a community member since 2013. John has been a miner, journalist, and has worked for several startups including CoinPip and the DC-based blockchain advocacy group, the Chamber of Digital Commerce.

### 3.4 Human Resource Management of the Foundation

Qtum is committed to develop the most influential open source community. In order to ensure the smooth technical development, to maintain effective operation of the Foundation, and to differentiate from the traditional enterprise and other non-profit organization recruitment process, the Foundation will exercise a highly selective process to recruit for developers and form the management team.

#### Recruitment

The recruitment process is in accordance with “Competition, Merit, Experience” principle, which includes more than two interviewers and other investigations such as background screening, work experience, business interests, employment approval, and probation period.

Foundation management functions, such as finance, legal, taxation, etc., will be outsourced to third parties. The outsourced activities must be approved, including signing service agreement of resource outsourcing, by the Finance and Human Resource Committee and chairman.

Since the open source ecosystem community offers the most talented developers, the Foundation will recruit those industry experts as technical advisors. All related recruitment and compensation must include the sign up service agreement, as well as the approval of the Judgement Committee, the Code Review Committee and the Finance and Human Resource Committee.

#### KPI assessment





The Judgement Committee shall perform annual KPI assessment, including fund operations, Foundation management, community coordination, due diligence, and job rotations. The Community votes for the members of the next Judgement Committee; the members, except for chairman, are eligible for re-election (up to three terms).

Due to the various nationalities of developers, they are divided into two types: full-time and part-time. The foundation shall design policies for salary management and performance assessment system. The developers shall report their own progress in a timely manner. The Code Committee shall perform a KPI assessment of the developers' reports.

In addition, the Legal due-diligence process and ongoing due-diligence process shall be conducted on a yearly basis.

### **3.5 Risk Assessment and Decision-making Mechanisms of the Foundation**

In order to develop and refine the risk management system, the Foundation requires an annual sustainability assessment of Qtum. The assessment covers project quality, progress and application. For example, Smart Contract and Simple Contract implementations, threat identification analysis, internal control analysis, and risk identification and treatment.

The Foundation categorizes each incident according to its nature, such as the severity and scope of the impact, the likelihood of occurrence, and the impact on the amount of tokens. For the high priority incidents, which include general management and code-related events, the relevant committee is required to make decisions in a timely manner.

Regarding general management matters, the meetings are held by the members of the Foundation. Ultimately, the decision is made by the Finance and Human Resource Committee and the executive director.

For code-related events in the open source community and the use of funding, the decision-making process is usually done via voting. Members vote through the Foundation voting system based on the quantity and age of the possessed Qtum tokens. The voting results will be considered by the Judgement Committee when making the final decision.

In the case of emergency events (e.g., the events affecting the entire community), the Judgement Committee will use a bypass system to make decisions without prior voting results.

The Foundation will use the voting mechanism to avoid disputes. However, if disputes do arise, the Judgement Committee will weigh in the quantity and age of possessed Qtum tokens for the final decision.

### 3.6 Daily Operation Mechanisms of the Foundation

The Foundation will manage daily operations including, but not limiting to, the control activities listed below:

Control Objective	Control Activities	Control Owner
<b>Source Code Management</b>		
Source code management	The underlying architecture of open source code is stored on Github; only the core development members are authorized to modify and approve the code.	Source Code Review Committee
Source code modification	The requester can modify the source code only after the approval and authorization from the core development team.	Source Code Review Committee
Code development and modification	After authorization from the Source Code Review Committee, the developers can develop and modify the source code.	Source Code Review Committee
Code testing	The source code needs to be tested and documented in the testing report to ensure bugs are removed.	Source Code Review Committee
Code review	The source code needs to be reviewed by software tools and manual checks before deployment to the community.	Source Code Review Committee
Code deployment	Before deployment, the source code needs to be reviewed by the core developers.	Source Code Review Committee
Vulnerability fix	When vulnerabilities are identified, developers remediate and test the source code. The Source Code Review Committee reviews the code before deployment.	Source Code Review Committee
Drill testing	The Source Code Review Committee is responsible for performing drill tests periodically for the development and production environment.	Source Code Review Committee
Code modification permissions	For non-public product code, code modifications need to be approved and authorized by the Source Code Review Committee.	Source Code Review Committee
<b>Human Resource Management</b>		
Recruitment	Interviews need to be performed by more than two interviewers. The recruitment process is documented after an independent assessment and approval from the Finance and Human Resource	Finance and Human Resource Committee

Control Objective	Control Activities	Control Owner
	Committee.	
Background check (Due Diligence)	Recruitment of key developers and other key positions requires due diligence and retention of relevant documents.	Judgement committee
Professional service outsourcing	Professional service outsourcing, such as finance, legal and taxation, need to be approved by the Finance and Human Resource Committee. Third party selection process documentation and service agreements need to be retained.	Finance and Human Resource Committee
Salary and compensation	The compensation of Judgement committee members needs to be disclosed. The compensation of core developers and management staffs needs to be reviewed by the Judgement Committee. For others, compensation needs to be approved by their relevant committee.	Judgement Committee
<b>Marketing</b>		
New promotion channels	The Marketing and Public Relations Committee researches the direction, extensibility and promotion efforts of the newly added channels. Adding new promotional channels need to be approved.	Marketing and Public Relations Committee
Promotion service contracting	The newly added promotion services and channels need to be approved by the Marketing and Public Relations Committee before signing the service agreement.	Marketing and Public Relations Committee
Edit and review the promotion articles	The promotion articles need to be reviewed by the independent staffs before their release.	Marketing and Public Relations Committee
Crisis public relations handling	In the event of an emergency, the Marketing and Public Relations Committee needs to deal with crisis and to handle public relations before the Judgement Committee agrees to respond.	Marketing and Public Relations Committee
<b>Financial Management</b>		
Budget review	Funds operation budget should be made annually and reviewed by the finance department	Finance and Human Resource Committee
Contract draft	Terms of contract should be reviewed by	Finance and Human Resource



Control Objective	Control Activities	Control Owner
and review	Judgement Committee.	Committee
Contracting	Contract should be signed only subsequent to Judgement Committee's review.	Judgement Committee
Revenue recognition	Revenue mainly originates from PE and the crowdsale, bookkeeping is done by the finance department and reviewed by the Judgement Committee.	Finance and Human Resource Committee
Cost recognition	All costs should be accounted for and be reviewed by the Finance and Human Resource Committee	Finance and Human Resource Committee
Accounting treatment	Accounting treatments should be reviewed by the finance department and Human Resources; financial statements are prepared on a monthly basis.	Finance and Human Resource Committee
Funds reconciliation	Fund reconciliations should be performed between the general ledger and sub-ledgers on a monthly basis, and be reviewed by financial staff who are authorized by the Finance and Human Resource Committee.	Finance and Human Resource Committee
Disclosure	Periodic disclosures should be made to the Funds about the use of BTC and ETH, and the development of the Fund. The disclosure report should be reviewed by Judgement Committee.	Finance and Human Resource Committee
Outsourcing contracting	Contracts of certain functions that are outsourced should be approved by the Finance and Human Resource Committee.	Finance and Human Resource Committee

The Foundation needs to be assessed and audited by external parties, including the usage of raised funds, revenue, cost breakdowns and potential debts.

### 3.7 Financial Management of the Foundation

The financial management of the Foundation includes daily financial management and digital asset management. The financial management is outsourced, including developer's travel expenses, staff salaries, office expense, daily operation expenses, etc. Digital assets are managed by the Judgement Committee or other authorized personnel, including wallet management, transferred digital assets, other digital currencies switches, digital currency withdrawals, etc.

- **Funding source**

The specific financial and business requirements that will be evaluated differently from other segments are typically in the early stages of development and may not be



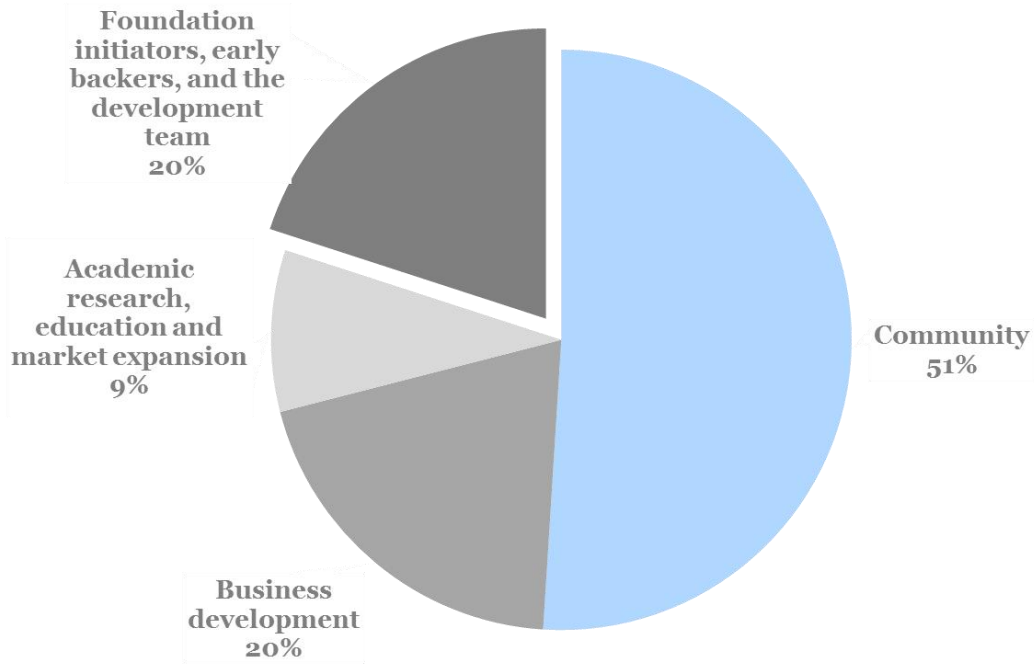
generating significant revenue. The major income is from seed round investment and the Crowdsale. Donators need to hold Qtum tokens in order to be authorized to use Qtum and its DApp.

- **Initial Qtum token allocation**

80% of the tokens will be eventually allocated the community; the remaining 20% will be allocated to the foundation initiator, early backers, and the development team. Please refer to Figure 1.

Percentage	Usage	Explanation
<b>51%</b>	Crowdsale	The fund raised in the crowdsale will be used for the operation of the Foundation, including development, administration, marketing, financial and legal consultancy, etc.
<b>20%</b>	Foundation initiators, early backers, and the development team	Foundation initiators, early backers and the development team are rewarded with Qtum tokens due to the effort, resources, and the technology they contributed to the development of Qtum.
<b>20%</b>	Business development	Select the appropriate industries to implement the Qtum blockchain technology, including strategic planning, project support and token swap.
<b>9%</b>	Academic research, education, and market expansion	The fund will be used for sponsorship of academic research, education materials for developers, raising awareness of the Qtum technology, and contribution to open source communities, etc.

### QTUM TOKEN ALLOCATION



Year 1

Figure 1

We plan to allocate the 29% (Business development 20% & Academic research, education, and market expansion 9%) to serve the community in the next 3-4 years (please refer to Figure 2). Ultimately, 100% tokens will be allocated to the community so that Qtum can become a truly open source community. Financial reports will be shared with the community regarding the usage of this 29%, and wallet addresses will be published.

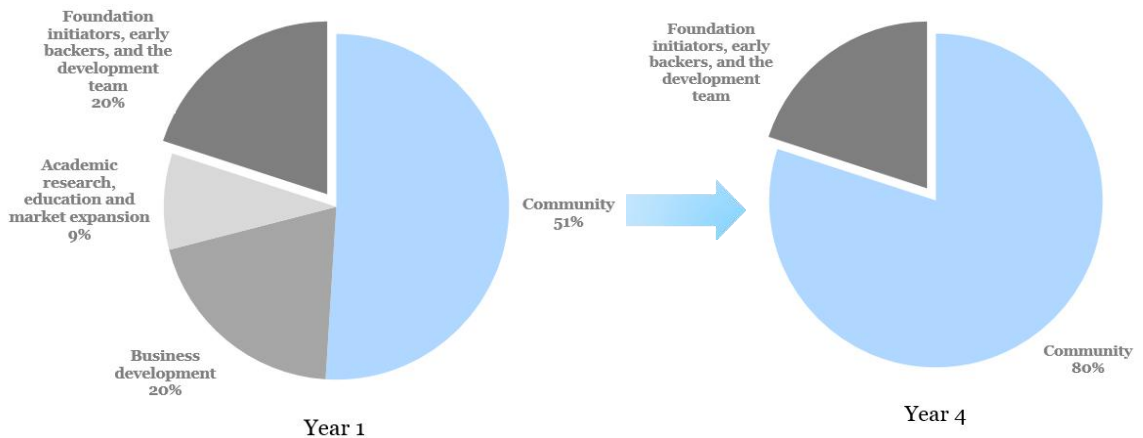


Figure 2



Percentage	Usage	Wallet address
10%	Business implementations	to be announced
10%	Token exchange	to be announced
9%	Academic research, education, and market expansion	to be announced

- **Restriction on the use of the funds**

The funds listed in the above wallet addresses shall be used based on the open and transparency principle. A trusted custodian institution monitors the usage of the digital assets and shares with the community periodically.

The usage principle of the fund obtained from the crowdsale:

- ✓ Expenditures over 50 BTC must be approved by the Finance and Human Resource committee;
- ✓ Expenditures over 100 BTC must be approved by the Judgement Committee.

- **Financial planning and execution report**

Quarterly, the Finance and Human Resource Committee shall develop financial planning and discuss financial performance of the previous quarter to form an off-chain financial report, which is then submitted to the Judgement Committee for review.

- **Digital assets management**

The digital assets belonging to the Foundation shall be managed by the Finance and Human Resource Committee or authorized personnel. The security and accuracy of digital assets are ensured by multi signature technology. All the income in fiat currency must be converted to digital currency in a timely manner and be deposited into a digital wallet. The funds of the Foundation shall not be deposited into personal accounts.

- **Digital wallet management**

Based on the independence principle, the Foundation's digital wallet shall be protected by multiple signature technology (3 of 4) mechanism. Adding new digital signatures must be approved by the Finance and Human Resource Committee.

- **The distribution and management of Qtum tokens**

Ownership of tokens refers to the right to use the Qtum DApps and the blockchain.



- **Disclosure**

On an annual basis, the Foundation shall disclose community matters, including status of development, operations of the public chain, and the usage of tokens, as well as whether the foundation operates in accordance with the governance policy.

### **3.8 Other Matters and Legal Affairs**

- **Legal affairs**

The Foundation is established in Singapore. All legal matters must seek advice from a lawyer who practices the local law.

- **Disclaimer**

The Foundation is a business entity that will transform into a non-profit organization. Participants in the crowdsale are given access to Qtum. The purchaser understands that there is neither expressed nor implied warranty with Qtum to the extent permitted by law, and that Qtum is purchased on an “as is” basis. Purchaser also understands that Qtum will not provide any refund under any circumstance.

- **Dispute resolution term**

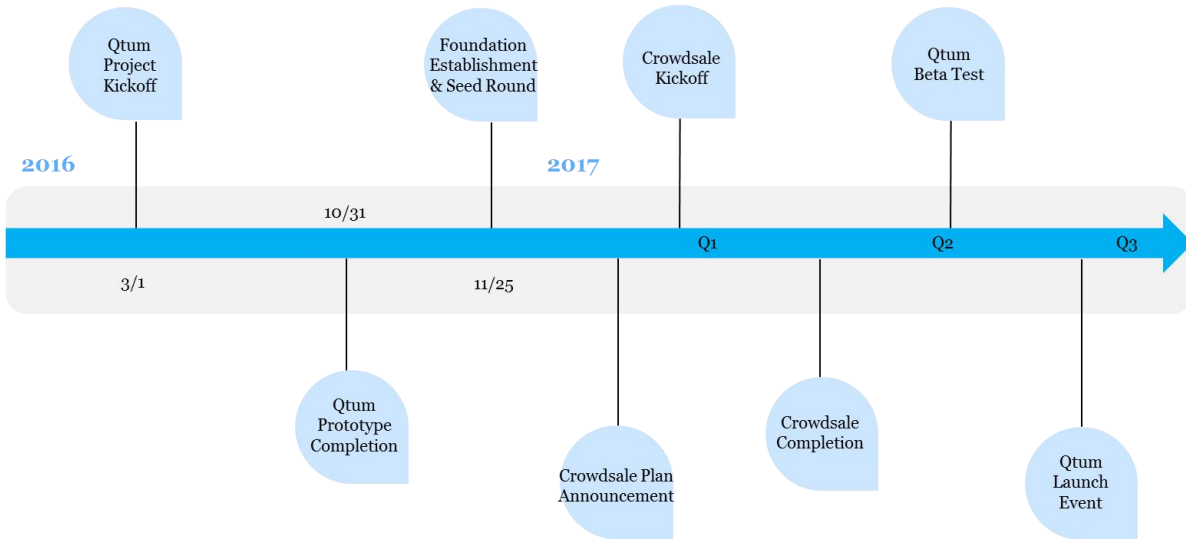
For disputes, the parties shall be settled based on agreement. In the case that no settlement is reached, each party can further dispute via legal means.



## 4. The Implementation and Iterations of Qtum

### 4.1 The Qtum Blockchain Implementation Timetable

#### *Qtum Project Timeline*



The Qtum project key milestones include:

- Qtum project kickoff: the project was officially started by its co-founders - Patrick, Neil and Jordan in March 2016;
- Qtum prototype completion: the Qtum development team completed the development of Qtum blockchain prototype in October 2016;
- Foundation establishment & seed round investment: The Qtum Foundation was registered as a non-profit organization in Singapore in November 2016. The seed round raised over one million dollars from early backers including Ethereum founder Anthony Di Iorio, OKCoin CEO Star Xu, BitFund founder Xiaolai Li and Fenbushi partner Bo Shen;
- The crowdsale plan announcement: to announce details of the crowdsale, including timing, method, bonus structure, fund security, etc;
- The crowdsale: to render the crowdsale based on the announced timetable and rules;
- Governance structure ready: to release the official governance statutes in the second quarter of 2017;
- Testnet completion: to release the testnet in the second quarter of 2017;



- Qtum launch event: to launch the Qtum Blockchain mainnet in the second or third quarter of 2017.

## 4.2 The Qtum Blockchain Crowdsale Plan

Users of Qtum will need to hold and use Qtum tokens for the designed functions of Qtum. The usage, or consumption, of a certain quantity of Qtum tokens is required to run the distributed applications on the Qtum Blockchain.

Qtum tokens will be fully generated upon the initial launch of Qtum and be held and owned by the Foundation.

The crowdsale details will be announced later in the crowdsale terms via Qtum’s crowdsale website.

Participation in the Campaign is not risk-free. See PROSPECTUS Chapter V “Risk Factors” for details.

For specific rights and obligations of the participants, please refer to PROSPECTUS : Chapter III & Chapter IV.

## 4.3 Future Iteration Plan of the Qtum Blockchain

For the continuous development of blockchain technology, the future iteration plan includes code iterations and business application iterations.

- **The Qtum underlying architecture iterations**

The following non-exhaustive scenarios illustrate when a system upgrade shall take place.

- ✓ Source codes vulnerabilities are identified;
- ✓ Significant impact on users funds;
- ✓ Severe security problems affecting the safety of the system.

For minor bugs, system shall be patched by the Source Code Committee directly.

- **Business application iterations**

The Qtum blockchain is an open source project committed to connect the blockchain and real world by innovation of technology and conception. Therefore, in the practical business implementations, the Foundation shall cooperate with appropriate third parties for application iterations, which shall be led by third parties and supported by the Foundation.



## 5. The Qtum Blockchain Applications

### 5.1 Decentralized Applications (DApp)

Decentralization is one of the characteristics of the Qtum blockchain. The Qtum blockchain develops different modules for different systems and users to simplify the preparation of development and to facilitate the DApp development. Furthermore, we introduce the Go Mobile strategy so that ordinary Internet users can experience the values brought by the blockchain technology.

With the introduction of incentive mechanisms and sharing economy, the Qtum blockchain will change the current application market and business model. The Qtum DApp marketplace can include decentralized social network, storage, DNS, and computing services.

### 5.2 Industry Oriented

Qtum provides support for business development by using industry focused consensus mechanism and incorporating regulatory requirements.

For example, The Qtum blockchain, with its unique approach to integrating off-chain factors while operating smart contracts, constitutes a sophisticated solution that uses new technology to tackle the requirements of financial institutions.

Qtum also can support many industry application requirements, such as Finance, Logistics, Supply chain, Social and gaming, Charity, Digital assets, Stocks, etc. Based on Qtum, smart contracts and Master Contracts can support more complex business logic and broader industries via Turing complete code language.

For more cases, please refer to the Chapter 6.

### 5.3 Go Mobile Strategy

Currently, blockchain-related development is mainly conducted on PCs. The Go Mobile strategy will help to introduce blockchain technology to ordinary Internet users and facilitate large implementation of blockchain technology.

In Qtum's open environment, we not only support and promote the Go Mobile strategy, but also provide mobile services with third party developers, including mobile wallet, mobile DApp, mobile smart contract app, etc.

The Qtum blockchain development team plans to set up a DApp store and to integrate blockchain technology, digital currency and the existing Internet applications (e.g., Wechat, cloud services). The Qtum team has released projects, such as Spring Email and Qloha, in the community. The goal is to turn each email address into a digital wallet.



## 6. Business Use Cases

### ***Case I: Blockchain Implementation in Smart Contracts***

Augur, a fully open-source and decentralized prediction market platform, was introduced in 2015 on Ethereum. It offers a better development platform for rapid deployment and utilizes blockchain technology to execute smart contracts.

On Augur, anyone anywhere can instantly create a market using any topic (e.g., who would be the winner of next US Presidential Election) with no need for centralized approval, can freely participate in all markets, and can save a large amount of fees for participants. Another important advantage is the reduced possibility of fraud and counterparty risk. Monetary exchanges on the platform are strictly regulated by smart contracts – a distributed oracle system that prevents claims from a false event result.

The underlying network unit utilized by Augur is known as reputation (or REP), which is used by the platform's referees to report event outcomes, while Bitcoin and Ether (Ethereum's internal currency) is used for market speculations.

Augur can be used as a distributed oracle system, allowing other smart contracts to propose questions and to discover information about the real world without having to trust a single person, AI or organization.

### ***Case II: Blockchain Implementation in Product Management***

Putting the unique IDs on the blockchain can create a transparent supply chain, which solves issues relating to counterfeit products via tracking and tracing merchandise, communication and cooperation among different parties in the supply chain, and supervision by government agencies.

A Product Management platform built on blockchain, called VeChain, was launched in early November 2016.

VeChain focuses on anti-counterfeiting, supply chain management, asset management and client experience enhancement by putting unique IDs on the blockchain and embedding each product with an Near Field Communication ("NFC") chip, Radio Frequency Identification ("RFID") tag or Quick Response ("QR") code – all of which can verify whether an item is genuine. VeChain provides an opportunity for different enterprises to easily create, manage, maintain and update shared data.

VeChain also introduces the function for making a connection among the different IT systems of various parties that operate on the supply chain.



---

### ***Case III: Blockchain Implementation in Property Mortgage Valuation***

Blockchain technology strengthens data traceability and ensures data accuracy by creating and transmitting cryptographic information via the Distributed Ledger Technology (DLT).

Bank of China (Hong Kong) (“BOCHK”), a leading listed commercial banking group in Hong Kong, announced the launch of Blockchain technology for property valuation. The bank completed the first case with its partnered surveyor on the 28<sup>th</sup> of November 2016.

The new technology speeds up the valuation and loan approval processes and enhances operational efficiency, representing a major step in fostering the development of financial technology in Hong Kong. As a result, banks cut costs by streamlining the validation process of valuation paper reports.

Currently, BOCHK is partnering with two property surveyors. To promote the application of Blockchain technology and to enrich the content of the property valuation information, BOCHK plans to invite more surveyors and other banks. The regulator, Hong Kong Monetary Authority (HKMA), is pleased to see the materialization of the DLT value proposition, as well as the proof-of-concept work that involves DLT in the actual banking business.

BOCHK plan to further its effort by exploring and studying applications of Blockchain in areas including trade finance, digital ID management and cross-border payments.

### ***Case IV: Blockchain Implementation in Mobile Bill Platform***

Blockchain technology can provide high durability, reliability and longevity, transparency, and immutability. These attributes can be used to build up a platform that allows mobile bill transactions.

On 11<sup>th</sup> November 2016, China Zheshang Bank (“CZBank”) announced that it will launch a blockchain-based Mobile Bill platform in January 2017.

CZBank utilizes this technology to build up a Mobile Bill platform that allows merchants and retail customers to issue, receive, negotiate, sell/purchase and pay bills.

CZBank believes this service, which is the first of its kind in China, will help its customers to increase efficiency in wealth management and to reduce costs associated with the process.



### ***Case V: Blockchain Implementation in Securities Trading***

On the 29<sup>th</sup> of November 2016, the German central bank, Deutsche Bundesbank, being the most influential member of the European System of Central Banks (“ESCB”) due to its strength and former size, unveiled a functional prototype of a Blockchain technology-based settlement of securities.

Jointly presented with Deutsche Borse, the marketplace for the trading of shares and other securities, the prototype represents the first successful result of a collaborative research project between the two institutions (based on a conceptual study that is not market-ready).

The prototype is designed to provide technical functionalities needed in the settlement of securities, including the delivery-versus-payment mode for centrally-issued digital tokens and the pure transfer of either digital tokens or digital securities. The two institutions plan to further develop the prototype over the next few months to analyze the technical performance and the scalability.

### ***Case VI: Blockchain Implementation in Logistics***

In early November 2016, the largest shipping port, Port of Rotterdam, together with ABN Amro, Delft University and the Netherlands Organization for Applied Scientific Research, announced that Blockchain technology will be introduced and tested in logistics.

Over the next two years, consortium members will test applications for sharing logistical and contractual information between parties. According to Delft University, the project will move forward in conjunction with a separate Blockchain initiative pursued by the Dutch Ministry of Economic Affairs. The involved consortium members are not alone in exploring the technology for logistics use. The project’s organizers expressed that the work will focus on real-world applications and uses.



---

## Appendix 1 Glossary

1. Bitcoin: A cryptocurrency and a payment system invented by an unidentified programmer, or group of programmers, under the name of Satoshi Nakamoto.
2. Ethereum: A public blockchain-based distributed computing platform, featuring smart contract functionality.
3. Value Transfer Protocol: A protocol that allows the secure transfer of value from peer to peer.
4. Internet of Things: The Internet-connected of physical devices, vehicles, buildings, and other items, embedded with electronics, software, sensors, actuators and network connectivity that enables these objects to collect and exchange data.
5. Oracle: A machine or a program which can select appropriate data inputs based on pre-defined rules.
6. Data feeds: Contracts on the blockchain that serve data requests by other contracts.
7. PoS: Proof of Stake is a consensus algorithm that relies on coin ownership to achieve distributed consensus.
8. UTXO: Unspent Transaction Output.
9. Smart Contracts: Smart contracts are computer programs that autonomously execute the terms of a contract.
10. Altcoin: Altcoins are cryptocurrencies other than Bitcoin.
11. PoW: Proof-of-Work is a consensus algorithm that produces a piece of data which is difficult to produce but easy for others to verify and which satisfies certain requirements.
12. Public chain: A blockchain which can be used and accessed by the public.
13. Ethereum Virtual Machine: EVM is a virtual machine designed to be run by all participants in a peer to peer network. It will only execute code when it receives a message verified by a digital signature.
14. IPoS: Incentive Proof of Stake, a combination of PoS, incentives, and estimation of online nodes.
15. Hard-fork: A permanent divergence in the blockchain, commonly occurs when non-upgraded nodes cannot validate blocks created by updated nodes that follow newer consensus rules.
16. DAO: A decentralized autonomous organization, running through rules encoded as smart contracts.
17. Turing complete language: A language that can simulate the computational aspects of any real world general-purpose language.



---

## References

- [1] <https://en.bitcoin.it/wiki/Category:History>
- [2] <https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf>
- [3] <https://github.com/bitcoinbook/bitcoinbook>
- [4] <https://github.com/ethereum/wiki/wiki/White-Paper>
- [5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, <https://www.bitcoin.org/bitcoin.pdf>
- [6] James Gong, 2016, Blockchain Society - Decoding Global Blockchain Application and Investment Cases
- [7] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015, <https://github.com/DavidJohnstonCEO/DecentralizedApplications>
- [8] Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, <http://ethereum.org/ethereum.html>
- [9] Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, <http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf>
- [10] PriceFeed Smart Contract, 2016, <http://feed.ether.camp/>
- [11] Nxt, 2013, <http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt>
- [12] <http://chainb.com/?P=Cont&id=2863>
- [13] <http://chainb.com/?P=Cont&id=2856>
- [14] [http://www.bochk.com/dam/bochk/desktop/top/aboutus/pressrelease2/2016/20161128\\_01\\_Press\\_Release\\_SC.pdf](http://www.bochk.com/dam/bochk/desktop/top/aboutus/pressrelease2/2016/20161128_01_Press_Release_SC.pdf)
- [15] <http://tech.sina.com.cn/i/2016-08-09/doc-ixutpf1573966.shtml>





---

## Revision History

Version	Date	Author	Summary of changes
1.0	Feb 9 2017	Qtum Foundation	Initial release