



A Perfect Security and Speed Solution for Exchanges

White Paper (Beta)

Version 1.7.1

The final white paper published by the official website shall prevail

Contents

Abstract	4
I. Profile of the Digital Assets Market.....	5
1.1 Current Status of the Digital Assets Market	5
1.2 Current Status of Digital Asset Exchanges	5
II. BITARK KO Solutio —the Technical Solution	8
2.1 A Financial-level Security Trading Platform	8
2.2 High-speed Trading Performance	13
III. BITARK Multi-service Extension.....	14
3.1 Artificial Intelligence Investment Advices and Customer Service	14
3.2 Transaction Records Open to the Block-chain	15
3.3 Active Wealth Management.....	16
3.4 Building of Currency Platforms	16
3.5 Crowd Sale Services	16
3.6 Legal Currency Channels	17
3.7 Community Token Connection.....	17
3.8 Merchant Payment Service	17
IV. BITARK Token Design and Merchandise Planning.....	17
4.1 Token Design.....	17
4.2 The Role of Token and Its Return Mechanism	18
4.3 Distribution Ratio and Sales Details of Tokens	19
4.4 Fund Use Plan	20
V. Course & Plan & Team & Consultant	22
5.1 Course	22
5.2 Future Development Plan	22
5.3 Core Team	23
5.4 Project Consultants & Investors.....	25
VI. Risk Warning and Disclaimer	29
6.1 Disclaimer.....	29
6.2 Risk Warning.....	31
Attachment 1	33

Attachment 2	38
--------------------	----

Abstract

BITARK KO SOLUTION, the first hacker immune trading technology, is designed to provide exchanges in the world with a solution which is completely immune to hackers and can serve ultra-high frequency trading for about tens of millions of transactions per second. It only takes 7-10 sets of servers to serve 224 countries and regions in the world.

BITARK KO SOLUTION is a perfect combination of all hardware and software, from the basic CPU, to the key machine, the operating system, and to the key management system, user management system, distributed disaster-recovery management center and other system software. It is a solution to provide ultimate security for digitally encrypted currency exchanges!

We've created a model exchange — BITARK, and will start an activity this summer called a million dollar hacking reward to prove the reliability of our technology.

BITARK Exchange has started the layout and registration of the EU system which entered the testing phase of on-line deployment in January 2018. After BITARK comes online, it will develop and deploy artificial intelligence customer service and investment management.

I. Profile of the Digital Assets Market

1.1 Current Status of the Digital Assets Market

With the ICO mania of block-chain, digital asset transactions show a blowout growth in the vitality and volume. According to the December 7 data of CoinMarketCap, a statistic website of the digital assets market, more than 1,000 kinds of digital asset currencies recorded in it register an aggregate value of more than RMB2700 billion, 270 times more than that in the beginning of 2017 (RMB10 billion).

1.2 Current Status of Digital Asset Exchanges

CoinMarketCap's December 7 data show that the number of exchanges worldwide has exceeded 7,185. Centralized digital asset exchanges are the mainstream of the current market models, with the following transaction process: the user needs to place legal tenders or tokens into the bank account or block-chain address of the exchange; after that, the exchange will conduct IOU accounting, like a bill of debt to be transacted between users; the user needs to submit a withdrawal application to the exchange; and until the withdrawal is achieved, the transaction really completes. Before the withdrawal, the user bears triple risks: exchange's security capabilities, digitally encrypted currency and legal currency

management capacity, and business operators' commercial morality. In the meantime, the mode can hardly meet the actual market demand in data turnover, response efficiency, accuracy and other core elements of an exchange. Many exchanges are faced with the lagged or dropped phenomenon caused by heavy load from the rapid growth of business, resulting in poor user experience.

There have been decentralized exchanges, like Ripple, BitShares and Openledger, built on block-chain in open source communities. Due to the low transaction efficiency and poor user experience in the decentralized exchange, it can not meet the market demand. Therefore, the demand for decentralized trading platforms is beginning to emerge, but exchanges like EtherDelta are far from meeting market demand.

With the rapid growth of global digital assets in the short term, huge benefits to participants have attracted a large number of new users. In the meantime, as ICO and other financing methods become popular, millions of dollars of new digital assets are created every day, leading to the rapid increase of transaction demand. The problems of the centralized trading platform have also attracted more people's attention. Among them, the urgent problems to be solved include:

1. Risk of intrusion and theft: centralized exchanges will be important targets of hacker attack because they are using general servers as hardware and the open source Linux operating system as software. Because of open-source software, server trusteeship, inside jobs and other reasons, the exchanges cannot avoid the disastrous consequence of hacker attack completely. Exchanges' Security issues take place almost every year. For example, the well-known Mt.Gox incident, which brought disastrous consequence, directly resulted in the collapse of the exchange and the loss of user assets. (Refer to attachment 1)

2. Vulnerability: Both centralized and decentralized exchanges are vulnerable to network congestion, DDOS or other attacks of service denial. Due to the existence of centralized nodes, in particular, the platform is subject to be a focus of attacks, which means a huge cost to avoid such attacks. The cost will be finally borne by users.

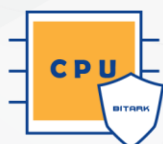
3. Loading risk: As all existing exchanges are using ordinary servers to build the platform, the larger the server cluster is, the lower the efficiency of the task execution will become. What's more, due to the lack of global distributed layout (data synchronization within server clusters is one of the major problems), currently all exchanges have poor loading capacities to meet the needs of the

market. For example, on December 1, 2017, the most bizarre slump occurred in the world's largest exchange Bitfinex, with many currencies declining by 90%, almost equal to zero. So far there is no evidence that this is artificially caused by the exchange. The possible reason is that the loads greatly exceed the affordability of the exchange, causing erroneous transaction data and triggering user selling. This kind of case becomes more common in recent years.

4. Decision-making risk: Decentralized exchanges often make decision-making mistakes in the execution of policies. Latent risks may be caused even if technological means are adopted to ensure property safety, which cost a lot of time.

II. BITARK KO SOLUTIO — the Technical Solution

2.1 A Financial-level Security Trading Platform



Hardware protection

customized CPU: layout from the basic computer hardware
the financial-level cipher machine: advanced key management technology
special USB-key: multiple security protection



Software protection

Independent operating system and transaction software
Combine software and hardware to provide multiple protection



Strategy protection

Distributed deployment: avoid data security risks
multiple authorization: eliminate the risks of internal transactions
the EU CC certification: authoritative security certification
Global hacker Competition: use facts to prove security

Three Kinds of Protection

The core requirement of the exchange is to ensure the security of asset storage and transactions. Based on a strong technical team, BITARK starts the layout from the bottom layer, combining software and hardware, to create a financial-level security solution — BITARK KO SOLUTION to ensure the security of the encrypted currency exchange.

All software has vulnerabilities in the field of computers! It is hence not reliable to protect storage security only by software. We will combine software and hardware to separate hackers with the financial -level security measures.

1. Hardware protection

1) Customized CPU: layout from the basic computer hardware.

The dedicated instruction set is designed independently, so programs running in the host must use our self-developed compiler, while hackers, using a common compiler to compile programs, ends up with nothing, which can fundamentally eliminate all possible intrusion.

2) The financial-level cipher machine: advanced key management technology

It is mainly used to realize data encryption/decryption, correctness verification of message sources, and key management

in the application layer of the host, which is an effective physical tool for the level of financial data security protection. It has a complete key management system that provides truly random keys generated by full hardware noise sources (other exchanges only provides pseudo-random keys) and can effectively prevent the active attacks on the communication channel. The cipher machine physically closes the sensitive information and makes it unreadable. The hardware chip has a self-destruction function when faced with dismantling. In compliance with FIPS 140-2 Level3 international standards, the machine maintains high security.

3) Special USBkey: multiple security protection

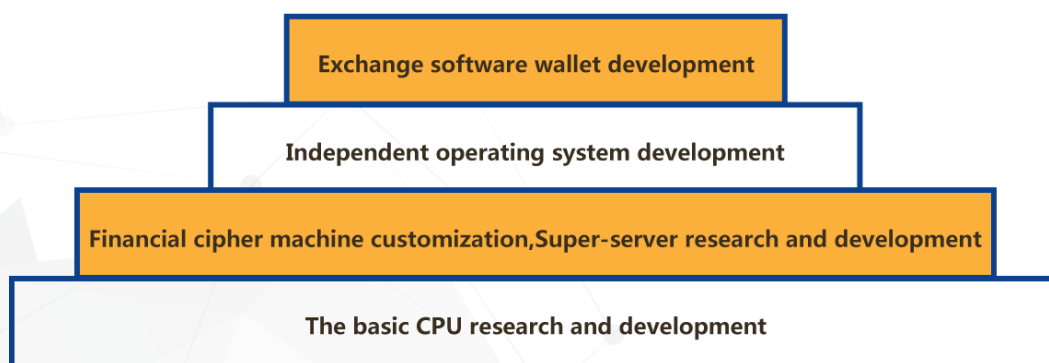
User's core security information and private keys can be physically isolated through a special USBkey, a cipher machine and other equipment. With a self-destruction function in each hardware chip and without the user's security equipment, the private key in the chip won't be obtained even if the hardware is stolen, which ensures the security of the user's assets and prevents all possible inside jobs.

2. Software protection

All operating systems and software of the exchange are non-open source software under independent development, such as wallet, trading system, key strategy management system, user

management system, decentralized storage management system, decentralized disaster-tolerant management center and so on. At the document and communication level, a number of encryption protection means, two-factor authentication mechanism and other cross protection systems shut the door of any opportunity to hackers.

At the document and communication level, we also have a number of encryption protection means to ensure that each layer is carefully guarded and no mistake could even happen.



BITARK Security Pyramid Model

3. Strategy protection

1) Distributed deployment: avoid data security risks

With a decentralized management mode, the system employs distributed deployment, multi-signature and bank authorization mechanisms to ensure security. In specific, the server uses distributed deployment and multi-node data backup to ensure data security and avoid the security risks caused by geographical

environment emergency situations

2) Multiple authorization: eliminate the risks of internal transactions

The exchange uses multi-signature and bank authorization operation management mechanisms to avoid inside jobs.

3) EU CC certification: the most authoritative security certification

As for hardware and software security, we have invited the top domestic security experts to develop CC certification plans for us. The basic work of the domestic security certification has been deployed and the EU security certification has also been included in the plan. We will use relative certification to support BITARK's impeccable security. (For Common Criteria, referred to as CC, see attachment 2)

4) Global hacker competition: use facts to prove security

BITARK will carry the block-chain transaction security technology, developed by the team, to participate in the new global hacker competition and carry out the "Million Cash Exchange Challenge" activity to prove the security performance of our core technologies with facts!

2.2 High-speed Trading Performance



Dedicated server



High-speed distributed algorithm



The basic private key intelligent identification technology

Three High-speed Experience

1.Dedicated server

The ultra-high performance server, with an optimized CPU instruction set in the chip, achieves over-speed calculation through circuits. Frequency is replaced with bandwidth within the server to optimize communication. The server groups are divided physically, and computing and encryption/decryption are allocated to specific machines, so as to avoid the problem of low efficiency caused by constantly increasing servers. BITARK's dedicated server is equipped with independently developed 128-core CPU, 256G memory and 2 Gigabit Ethernet ports. The transaction speed of BITARK transaction system in current tests have reached 1 million deals/ second, without any lagged and crashed phenomenon, which meets the high-frequency trading demand of the increasing users.

2.High-speed distributed algorithm

The server groups are divided physically, and computing and encryption/decryption are allocated to specific machines, which can

greatly improve working efficiency. 7 to 10 servers will be enough to complete the global layout and offer service.

3.The basic private key intelligent identification technology

With the private key dispensed with encrypting, saving and invoking unlike that in other exchange, we no longer need to waste computing resources in high frequency encryption and decryption. That allows our servers to easily exceed other exchanges that use common business hosts and Linux system in speed.

III. BITARK Multi-service Extension



Dual-core drives eight services extension

3.1 Artificial Intelligence Investment Advices and Customer Service

In 7*24*365 block-chain market, customers spend a lot of time and efforts in reading the tape, trading stock and so on. In this

regard, we will use artificial intelligence and rely on the exchange data to develop artificial intelligence investing and consulting tools to achieve intelligent stock-trading. At that time, the customers can use the traditional way, or set their own smart assistant to facilitate operation and greatly save their trader time. It will also provide a series of intelligent investment strategies, for example, by comparing the rate of return, following other intelligent assistants to achieve the best balance of income and time.

We have developed a prototype for the artificial intelligence customer service, and shortly after the operation, the exchange can complete the deployment of artificial intelligence customer service through a short period of iteration. Our Artificial Intelligence customer service primarily offers answers to trading questions and fundamental Q&A on digital encrypted currencies.

3.2 Transaction Records Open to the Block-chain

All records of BITARK exchange will be made public through block-chain technology, mainly including the following aspects:

1. All transaction records are distributed through block-chain technology.
2. A number of credible main chains will be used for cross and multiple transaction records.
3. BITARK exchange can provide an external API interface for

transaction records.

3.3 Active Wealth Management

BITARK has received the support of many digital asset funds and will form some high-quality income items, whose yield will be subdivided in accordance with their corresponding risk weight, forming short, medium and long-term encrypted monetary asset portfolios based on customers' risk appetites, and dynamically matching investment needs of fixed income + floating income for various investors at all stages.

3.4 Building of Currency Platforms

The OpenBazaar platform is the only available B to C online store in the blockchain area, but its webpage loads very slowly and the user experience is bad. We will build an exchange-integrated Crypto-Commerce platform that will not only enhance the consumer experience, but also complete payment by using any tokens that are on the BITARK exchange. So the products can be sold around the world under simple block-chain business logic.

3.5 Crowd Sale Services

We will help customers to design their products or brands, and complete their crowd sale. Their token will be listed on the BITARK exchange. So crowd sale services and currency platforms can be echoed to complete the business closed-loop.

3.6 Legal Currency Channels

BITARK team has developed an easy OTC trading system ,which allows OTC deal-making fast,and the value exchange between digital assets and legal tender in the best possible way.

3.7 Community Token Connection

A token community will come into being by establishing a sound community token reward rules and connections will be made to digital currency exchanges to promote the flow of digital assets and the construction of block-chain ecosystem.

3.8 Merchant Payment Service

Connections will be made to global online and offline merchants that offer token payment to accelerate the historical process of encrypted currency payment.

IV. BITARK Token Design and Merchandise Planning

4.1 Token Design

BITARK issues cap the amount of 10 billion BARK tokens, and promises to never issue new ones.

BARK is a standard ERC20 token. The functionality of the

ERC20 is provided by the StandardToken contract, while the basic mathematical functions, including security detection, are provided by the SafeMath contract.

4.2 The Role of Token and Its Return Mechanism

1. Deduction of the platform transaction fees

Platform users who pay transaction fees with BARK can enjoy the relevant preferential policies. The specific implementation standard is shown as below.

	1st year	2nd year	3rd year	4th year	5th year
discount	50%	25%	12.5%	6.25%	none

2. The "fuel" to access the platform

In order to ensure scalability, the platform will open API interfaces, hardware services and a range of access services to improve its own ecosystem. When accessing to the existing currency exchanges, BARK will act as the role of "fuels".

3. Return Mechanism

When the exchange goes into operation, we will repurchase BARK with an amount of tokens no less than X% of the net profits of the entire project every quarter based on the following standard and burn them out to benefit all the BARK holders. The repurchase and burnout records will be released as soon as possible and users are allowed to check them through the block-chain browser so as to

ensure openness and transparency. The repurchase and burnout will proceed until the half of BARK is left.

	first quarter	second quarter	third quarter	fourth quarter	from the fifth quarter
Net profit repurchase rate	40%	30%	20%	10%	10%

From then on, we will quarterly include 10% of the net profit of the entire project into the Community Development Fund which operates in a DAO (Decentralized Autonomous Organization) model. Anyone can launch a proposal to help BITARK develop. If the proposal is approved, the corresponding funds will be disbursed immediately.

4.3 Distribution Ratio and Sales Details of Tokens

BITARK will crowd-fund on the official website of BITARK on January 25, 2018 European time. Token distribution ratio is as follows:

Time: BITARK crowd-funding time is tentatively scheduled on January 25, 2018 to February 5, 2018 (end time), European time.

Crowd-funding: 15% of BARK (i.e. \$ 1.5 billion) is used for crowd-funding, with an exchange ratio: 1ETH = 40000BARK and the crowd-funding goal of 37500 ETH;

Policy Committee: 10% of BARK (i.e. 1 billion) is used to

stimulate marketing and foundation construction etc. and will be released 20% per month;

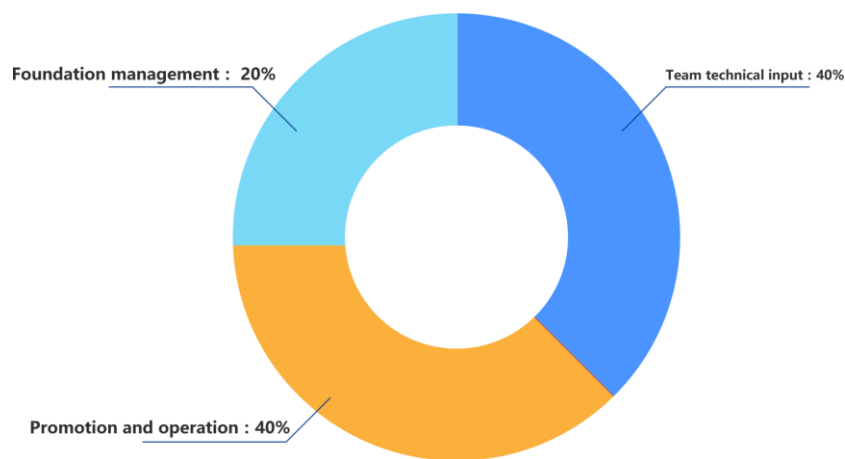
Advisory Team and Private Equity: 10% of BARK (i.e. 1 billion) for early investors will be locked up for 6 months after public crowd-funding.

BITARK Team: 15% of BARK (i.e. 1.5 billion), will be locked for 12 months after public crowd-funding.

Token Burnout: 50% of BARK (i.e. 5 billion) will be used for the destruction of the system's fixed-income ratio until all is burnout. BARK will be listed on a number of trading platforms after the end of burning.

4.4 Fund Use Plan

As for the fund from public offering, 40% will be used for team building, product development and hardware investment; 40% will be used as operation and promotion funds to ensure rapid access to the market and accumulate customers; 20% will be used as the reserve and managed by BITARK Foundation.



1. Technical input for the team:

Stage 1: complete the deployment of data center in Hong Kong, Singapore and Europe;

Stage 2: complete the integrated deployment in the United States and Australia, and establish the European R & D center at the same time.

2. Promotion and operation

- 1) Cooperate with existing token projects;
- 2) Cooperate with new projects;
- 3) Cooperate with traditional financial markets.

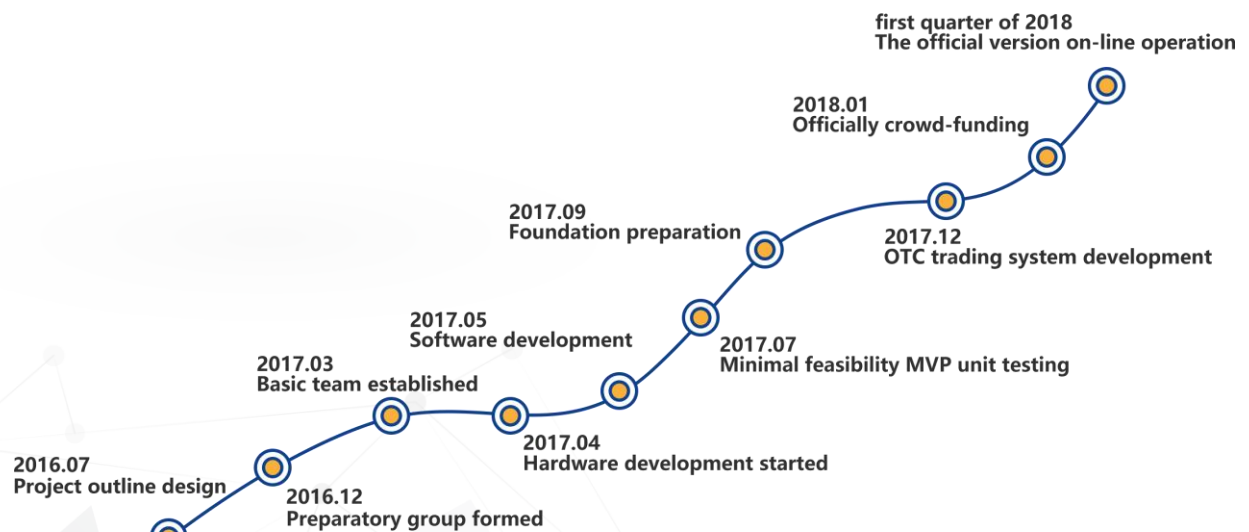
3. Product program

The project will offer all the financial services required by the traditional markets, such as spot commodity, future goods, leverage, index futures and other products, as well as explore and develop

products and services that are suitable for the block and might emerge in the future.





V. Course & Plan & Team & Consultant

5.1 Course



Roadmap

5.2 Future Development Plan

-  **Stage1, 2018.01**
 Online OTC market
 High-speed bidding trading platform (beta)
 Mainstream currency(BTC, ETH and so on) transactions testing
-  **Stage2, 2018.03**
 IOC platform (beta)
 Officially open high-speed bidding trading platform
 Open mainstream currency(BTC,ETH and so on) transaction
-  **Stage3, 2018.06**
 Officially open ICO platform
 Provide ICO distribution services, raise fund for the top currency and tokens
 Open more transaction currencies
 EOS,IOTA,QTUM,NEO,XRP,LTC and so on on-line APP and Client
-  **Stage4, 2018.12**
 Open option contract,Futures contract and Structured derivatives transaction

Future Development Plan

5.3 Core Team

Li Yuchen

Bachelor of Computer Science and Bachelor of Business Administration of Oakland Polytechnic University, an early participant in the Bitcoin community, a loyal fan of Ethereum community, with in-depth research into the areas of blockchain and Internet of Things, and with many years of senior management experience in large-scale listed companies in China and Japan.

Li Ge

She holds a bachelor's degree in laws and worked in the

DACA Blockchain Association and micro-finance 50 forums. She organized the translation and publication of the first Chinese block-chain book "Blockchain: New Economy Blueprint and Introduction", organized more than 50 blockchain keynote speeches and academic exchange activities and participated in the planning and design of iCenter blockchain courses in Tsinghua University. She also participated in hosting the 2016 Micro-financial Summit Blockchain Theme Forum and 2017 Guiyang Digital Expo Block-chain Theme Forum. He has undertaken a number of operation and promotion activities for well-known blockchain projects.

Dingding

Bachelor of Computer Science and Technology of Sichuan University. He has led the communications equipment research and development of a large state enterprise, of which the individual achievement reached the top of the industry in the world. He has undertaken the research and development of several communication systems that are applied to the world's top 500 enterprises, governments, banks and state-owned large and medium-sized enterprises. He has a profound systematic study on cryptography, blockchain, Internet of Things, AI and Big Data.

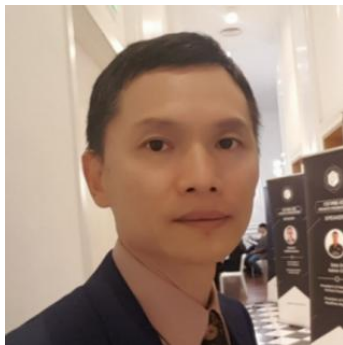
Zhao Liyu

Bachelor of Materials Forming and Control Engineering of Jiamusi University and graduate student of Macroeconomics of Tokyo University. He worked in Foxconn as a senior engineer and was responsible for supervising the development of a full range of devices for Apple mobiles. During his career as Manager of Southern China in Mitsubishi Electric, he was responsible for SMT mobile project management and new market development, and is keen on developing new technologies in the field of manufacturing.

Lin Jianfeng

Bachelor of Software Engineering of Xiamen University, keen on the development and application of open source technology, good at software engineering project management, and proficient in web technology, the underlying technology and blockchain technology. He worked in a Chinese commercial bank for years to offer technical support, responsible for software development and project management, and has rich experience in blockchain.

5.4 Project Consultants & Investors



Zhou Chaohui

He graduated from Fudan University, and is the Vice President of China DogeCoin Association, investment researcher of World Block-chain Foundation, a distinguished lecturer of iCenter of DACA & Tsinghua University and one of the keynote speakers at "Blockchain University Row" organized by the DACA Block-chain Association.

Addressed a number of speeches and lectures, and invested in more than 50 block-chain projects.

Editor in chief: "How to Invest in Digital Currency", "DOGE: The Most Valuable Life Wealth"

Involved: "Block-chain Development and Examples", "Block-chain technology and Practice of Application"

Editing: "ICO: 1 Minute Block-chain Investment", "Bit-coin Global E-commerce Platform — OpenBazaar"

Published PPTs: "Global Block-chain Investments", "Why Digital Currency Falls Recently", "Goodbye Bit-coin."



Cheng Maiyue

Director of Wuzhen Think Tank, former partner of Rocky Mountain Institute of the United States, senior fellow, sponsor of Wuzhen Think Tank, and consultant of China Development Financial (town development).

Mr. Cheng graduated from Fudan University, Beijing International Relations Institute and Wilson International School of Public Affairs, Princeton, USA, with a bachelor's and master's degree in international relations, economics and public policies. For more than 20 years, Mr. Cheng has worked in the World Bank headquarters, top transnational corporations in the energy and communications field and well-known international consultants. He has been working with Chinese government and large state-owned enterprises for a long time, and is active in economic and financial analysis, urban planning strategy, direct investment / private equity, entrepreneurial services and other fields.

In recent years, Mr. Cheng has participated in the project of "Reshaping Energy - China (Energy Vision 2050)" co-hosted by the Rocky Mountain Institute, Energy Research Institute of NDRC, Lawrence Berkeley National Laboratory and Energy Foundation (China) to promote strategic cooperation and seek low-carbon

development and policy ideas and solutions for green energy.



Bit-coin Ambassador — Li Weisheng

A royal accountant graduated from a university of the United Kingdom and a well-known international business consultant.

In 2004, on behalf of young overseas Chinese entrepreneurs, he was invited by the Chinese State Council to address a speech to the national leaders in the People's Great Hall in Beijing. He is a combination of speaker, investor, traveler, critic and writer. He is the only Chinese investor in the world who addressed speeches together with Jim Rogers and is the world's first person to travel around the world and make a documentary only with bit-coin. He was invited to address "Encryption Economic Storm" speeches at Summit Forums around the world. He is also the global advocacy ambassador of "Bit cloud", and the permanent chairman of World Block-chain Foundation (awarded the World Excellence Brand in 2017)



Deng Haitao

Graduated from the University of Nottingham, UK with a Master's degree in Information Technology and Management. As the investment director and chairman assistant of Dexun Capital, a China's well-known Angel Investment Enterprise, he founded Zhicheng Capital in 2014, and was awarded the title of "2015 New Youth Investors" and "2016 Shenzhen New Investment Agency" for his enterprise. He is an early participant in the Bitcoin project, a loyal fan of Ethereum community, and has a deep understanding of block-chain technology and applications. He was involved in the preparation of the formation of "DIC", a "Digital Asset Mortgage" project and served as the advisor for China's first unlisted equity block-chain project--"ShareX".

VI. Risk Warning and Disclaimer

6.1 Disclaimer

The use of this document is only for the purpose of communicating information and does not constitute a relevant opinion for participating in the BITARK project (BARK).

Any similar proposal or price will be made under a credible condition and subject to applicable securities laws and other relevant laws, and the above information or analysis does not constitute a specific recommendation for investment decisions.

This document does not constitute any investment advice, investment intent or abetting of investment in the form of securities. This document does not constitute nor should be interpreted as to provide any act of purchase and sale, or any act of inviting the purchase and sale of any form of securities, nor is any form of contract or promise.

BITARK project expressly states that the intended users have a clear understanding of the risk of BITARK. Once participating, it means they understand and accept the risk of the project and are willing to bear all the corresponding results or consequences for their own.

BITARK project expressly disclaims any direct or indirect loss caused by any participation in the BITARK project, including:

1. Economic losses due to user transactions;
2. Any errors, omissions or inaccurate information arising from personal understanding;
3. The loss incurred by the individual transaction of various types of block chain assets and any consequent acts.

BARC is an encrypted token used by the platform. BARC is not an investment, we can not guarantee that BARC will add value, and there even may be a decline in value in some cases. The incorrect use of BARC by the users may lead to the loss of the right to use

BARK and BARK itself. BARK is not a kind of ownership or right of control.

Controlling BARK does not represent ownership of the platform. BARK does not grant any individual any right regarding participation, control, or any decision making of the project.

6.2 Risk Warning

1. Security: The original intention of the project is to plan the trading platform based on the security concept. However, being vulnerable to damages caused by force majeure such as scientific and technological progress, and natural disasters, security itself remains a relative concept from time to time. Hereby we promise to take all the measures necessary to protect your assets.

2. Regulatory risks: Encrypted tokens are being or may be regulated by regulators in different countries and project participants may from time to time receive inquiries, notices, warnings, orders or rulings from one or more supervisors which may even suspend or stop BITARK development or related activity. As regulatory policies may change at any time, the existing state regulatory license or tolerance for open sale in BITARK may only be temporary. In different countries, BARK may be defined as virtual goods, digital assets or securities at any time, so in some countries, according to local regulatory requirements, BARK may

be prohibited from trading or holding.

3. Risks from the development of cryptography:

Cryptography is evolving and can not guarantee absolute security at any time. Cryptographic or technological advances may put cryptography-based systems at risk, including BITARK. This may result in the steal, theft, loss, destruction or devaluation of any BARK holder. To a reasonable extent, the project owner will take precautionary and remedial measures to upgrade the BITARK Agreement in response to any progress in cryptography. The future of cryptography and security innovations is unpredictable, and project parties and community members will do their utmost to adapt to the changes in cryptography and security.

4. Competition risks: The exchange is a highly competitive market with thousands of existing and planned exchange platforms, and the competition will be brutal. In this era, both start-up companies with good concepts and mature companies face the risk of competition, which is the driving force in the development process.

Attachment 1

List of Bitcoin Hacks (2012-2016)

Date	Organization Name	Intrusion Method	Quantity of Bitcoins Stolen	Loss
Jun. 2017	Bithumb	An employee's computer was hacked into	Unknown	\$870,000
Apr. 2017	Yapizon	Unknown	3831	\$5,300,000
Aug. 2016	Bitfinex	User wallets	119,756	\$66,000,000
Jul. 2016	Kraken	Some user accounts were broken through	Multiple kinds of digital assets	Unknown
Jul. 2016	Bitmex	User accounts were broken through	Unknown	Unknown
Jul. 2016	ItBit	User accounts were broken through	Unknown	Unknown
May 2016	Gatecoin	Hot wallet	Multiple kinds of digital assets	\$2,000,000
May 2016	SimpleFX	Mail system was attacked, and many fraudulent mails were sent to users.		Unknown

Apr. 2016	Yaykuy	Attacked and failed		Unknown
Mar. 2016	ShapeShift	inside job	Multiple kinds of digital assets	\$230,000
Mar. 2016	BitQuick	User name, phone number and mail information were stolen	None	None
Mar. 2016	Cointrader	Hot wallet	81 BTC	\$33,600
Jan. 2016	Cryptsy	Unknown	13,000BTC 300,000LTC	RMB 40,000,000 nearly
Jan. 2016	Bitstamp	Hot wallet	18,866	\$5,263,614
May 2015	Bitfinex	Hot wallet	About 1,500	About \$360,000
Mar. 2015	Exco.in	Cold wallet/inside job	Unknown	Unknown
Mar. 2015	Kipcoin	Cold wallet /inside job	3,000	\$690,000
Mar. 2015	796	Cold wallet /inside job	1,000	\$230,000
Feb. 2015	Bter	Cold wallet	7,170 BTC	\$1,750,000
Feb. 2015	Yes-BTC Taiwan	Unknown	Unknown	Unknown. Run-away
Jan. 2015	Bitstamp	Hot wallet	19,000	\$5,100,000

Jan. 2015	Cavirtex	User database was stolen	Unknown	Unknown
Dec. 2014	Blockchain.info (wallet)	User wallets (bug, R values)	267	\$101,000
Dec. 2014	Mintpal	inside job	3,700	\$3,208,412
Aug. 2014	Bter	Unknown. Hacker lurked for months	50,000,000 NXT	RMB 10,000,000 plus
Aug. 2014	Cryptsy	inside job	Multiple kinds of digital assets	\$6,000,000
Mar. 2014	Flexcoin (wallet)	Hot wallet	1,000	\$738,240
Mar. 2014	Poloniex	Code bug, user withdrawal to negative	12.3% of reserve fund	Unknown
Mar. 2014	Bitcurex	Unknown	10%~20% of capital	Unknown
Mar. 2014	Canadian Bitcoins	Intruded by cheating customer service staff into opening the security mode	Unknown	\$100,000
Mar. 2014	CryptoRush	Cold wallet /inside job	950	\$782,641
Jan. 2014	Mt.Gox	Hot/cold wallet/inside job	850,000	\$700,258,171

Dec. 2013	Blockchain.info (wallet)	2-factor authentication breach	800	\$800,000
Nov. 2013	Inputs.io (wallet)	Cold wallet /inside job	4,100	\$4,370,000
Nov. 2013	BIPS (wallet)	Cold wallet /inside job	1,200	\$1,200,000
Nov. 2013	PicoStocks	Cold wallet /inside job	6,000	\$6,009,397
Sep. 2012	Bitfloor	Unencrypted wallet data files were stolen	24000	\$250, 000
May 2012 Mar. 2012	Bitcoinica	Unknown	Unknown	Unknown
Mar. 2012	Linode (server co-location)	inside job	46,703	\$228,845
Aug. 2011	My Bitcoin	Unknown	780000	About \$ 800,000
Jul. 2011	Bitomat	Access right of wallet.dat was lost	17,000 BTC	About \$220,000
Jun. 2011	Mt.Gox	Security flaw	Unknown	Unknown



Attachment 2

Common Criteria

The **Common Criteria for Information Technology Security**

Evaluation (hereinafter referred to as **Common Criteria** or **CC**) is an international standard (ISO/IEC15408) for computer security certification. It is currently in version 3.1 revision 5.

Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs). Vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and critical infrastructure.

Key concepts

Common Criteria evaluations are performed on computer security products and systems.

- **Target Of Evaluation (TOE)** – the product or system that is the subject of the evaluation.

The evaluation serves to validate claims made about the target. To be of practical use, the evaluation must verify the target's security features. This is done through the following:

- **Protection Profile (PP)** – a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, as defined below), or the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products can focus on those certified against the PP that meets their requirements.

- **Security Target (ST)** – the document that identifies the security *properties* of the target of evaluation. The ST may claim conformance with one or more PPs. The TOE is evaluated against the SFRs (Security Functional Requirements. Again, see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.

- **Security Functional Requirements (SFRs)** – specify individual security **functions** which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, a SFR may state **how** a user acting a particular role might be authenticated. The list of SFRs can vary from one evaluation to the next, even if two targets are the same type of

product. Although Common Criteria does not prescribe any SFRs to be included in an ST, it identifies dependencies where the correct operation of one function (such as the ability to limit access according to roles) is dependent on another (such as the ability to identify individual roles).

The evaluation process also tries to establish the level of confidence that may be placed in the product's security features through quality assurance processes:

- **Security Assurance Requirements (SARs)** – descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the ST and PP, respectively.

- **Evaluation Assurance Level (EAL)** – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Normally, an ST or PP author will not select assurance requirements individually but choose one of these packages, possibly 'augmenting' requirements in a few areas with requirements from a higher level. Higher EALs *do not* necessarily imply "better security", they only mean that the claimed security assurance of the TOE has been more extensively verified.

So far, most PPs and most evaluated STs/certified products have been for IT components (e.g., firewalls, operating systems, smart cards). Common Criteria certification is sometimes specified for IT procurement. Other standards containing,

e.g., interoperation, system management, user training, supplement CC and other product standards. Examples include the ISO/IEC 17799 (Or more properly BS 7799-1, which is now ISO/IEC 27002) or the German IT-Grundschutzhandbuch.

Details of cryptographic implementation within the TOE are outside the scope of the CC. Instead, national standards, like FIPS 140-2 give the specifications for cryptographic modules, and various standards specify the cryptographic algorithms in use.

More recently, PP authors are including cryptographic requirements for CC evaluations that would typically be covered by FIPS 140-2 evaluations, broadening the bounds of the CC through scheme-specific interpretations.

Some national evaluation schemes are phasing out EAL-based evaluations and only accept products for evaluation that claim strict conformance with an approved PP. The United States currently only allows PP-based evaluations. Canada is in the process of phasing out EAL-based evaluations.

Testing organizations

All testing laboratories must comply with ISO 17025, and certification bodies will normally be approved against either ISO/IEC Guide 65 or BS EN 45011.

The compliance with ISO 17025 is typically demonstrated to a National approval authority:

- In Canada, the Standards Council of Canada (SCC) under Program for the Accreditation of Laboratories (PALCAN) accredits Common Criteria Evaluation Facilities (CCEF)
- In France, the Comité français d'accréditation (COFRAC) accredits Common Criteria evaluation facilities, commonly called Centre d'évaluation de la sécurité des technologies de l'information (CESTI). Evaluations are done according to norms and standards specified by the Agence nationale de la sécurité des systèmes d'information (ANSSI).

- In the UK the United Kingdom Accreditation Service (UKAS) accredits Commercial Evaluation Facilities (CLEF)
- In the US, the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accredits Common Criteria Testing Laboratories (CCTL)
- In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI)
- In Spain, the National Cryptologic Center (CCN) accredits Common Criteria Testing Laboratories operating in the Spanish Scheme.
- In The Netherlands, the Netherlands scheme for Certification in the Area of IT Security (NSCIB) accredits IT Security Evaluation Facilities (ITSEF).

Characteristics of these organizations were examined and presented at ICC 10.