XCash White Paper V2

Catalog

1.Background Introduction

1.1 Blockchain Technology

Since the 1970s, with the rapid development of cryptography technology, distributed networks, consensus algorithms, and hardware storage computing capabilities, the conditions for establishing a multi-master consensus mechanism through technology have matured. This is to solve mediation in multi-agent environments. Institutions trust risk, reduce transaction costs, enhance collaboration efficiency and provide new solutions.

In 2008, Nakamoto published a paper titled Bitcoin: A Peer-to-Peer Electronic Cash System, detailing how to create a set of decentralized Electronic trading system. This system does not need to be created on the basis of mutual trust between trading parties. For the first time, the establishment of a consensus mechanism between trading entities is achieved through technical means. Blockchain is the basic technology that constitutes such an electronic trading system.

Ethereum is another groundbreaking blockchain project following Bitcoin. It published a white paper in late 2013. Ethereum pioneered the integration of Smart Contracts and blockchains, and based on the establishment of a consensus mechanism between trading entities, it automatically triggered executable electronic contracts to solve the problems promised by transaction subjects. Promote the further development of blockchain industrialization and application.

EOS differs from Ethereum in its design philosophy. It tries to provide some common functions and modules that are required for different blockchain applications. EOS will be much more expensive than Ethereum in dealing with transactions. EOS uses the DPOS (delegated Prove of Stake) technology, which can achieve 10,000 to 1 million transactions per second under harsh testing conditions. However, this design has also made EOS an increasingly central trend.

The continuous development of blockchain technology and the accompanying upsurge of digital currency have triggered widespread attention from geeks to IT technology circles, financial fields, industrial economy, governments and public organizations, and media public opinion. Technology research, industrialization applications, and policy supervision have carried out extensive and beneficial exploration and practice. The mature application of blockchain technology still needs the thought of the multi-agent consensus coordination mechanism it brings, which will have a profound impact on social governance and business operations.

In the above background, the concept of XCash was born. XCash was originally designed to solve the centralization trend of current blockchains (such as EOS) using DPOS technology and the two types of problems like Ethereum's blockchain technology is easy to network congestion during transactions. Its design concept And technical principles are outlined in the following article.

1.2 Consensus Mechanism

The consensus mechanism is a core issue of blockchain technology. It determines the block generation rules in the blockchain, and ensures the integrity of each node, the fault tolerance of

the books, and the robustness of the system. Commonly used consensus mechanisms include PoW, PoS, dpos, Paxos, and PBFT. Based on the different application scenarios of the blockchain technology and the features of various consensus mechanisms, performance and efficiency, resource consumption, fault tolerance, and regulatory level can be evaluated and compared.

Good consensus mechanism functional components should have the following features:

Support multiple nodes to participate in consensus and confirmation;

Support independent nodes to verify the validity of relevant information submitted by blockchain network;

Prevent any independent consensus node from recording or modifying information in the blockchain system without confirmation from other consensus nodes;

Should be fault-tolerant, including non-malicious errors in the physical or network failure of the node, malicious errors in which the node has been illegally controlled, and uncontrollable errors in the node's indeterminate behavior.

Blockchain network protocols generally use the P2P protocol to ensure that each computer in the same network is equal to each other, and each node provides network services together. There is no "special" node. Different blockchain systems will develop their own P2P network protocols as required. For example, bitcoin has bitcoin network protocols. Ethereum and EOS also have their own network protocols.

1.3 Smart Contract

Introduced by Nick Szabo in 1995, his definition was: "A smart contract is a set of commitments defined in digital form, including agreements on which contract participants can execute these commitments." The nature and purpose of smart contracts.

The form of numbers means that contracts operate in the form of computer-executable codes. As long as the participants reach an agreement, the rights and obligations of the smart contracts are established by the computer or computer network.

Blockchain-based smart contracts can not only exert the advantages of smart contracts with low cost and high efficiency, but also can avoid the interference of malicious behaviors on the normal execution of contracts. Write smart contracts into the blockchain in a coded form, using blockchain technology to implement data storage, read, and execute processes that are traceable, transparent, and non-translatable. In addition, a state machine system constructed using a blockchain consensus algorithm can enable smart contracts to run efficiently.

The functional components of smart contracts include:

A, Development operating environment, including:

Provides programming language support, supporting integrated development environment if necessary;

Support contract content static and dynamic checks;

Provides carrier support for operations such as virtual machines;

For smart contracts interacting with external data of the blockchain system, the scope of influence of external data sources should be limited to the scope of smart

contracts and should not affect the overall operation of the blockchain system.

B, Storage environment, including:
Preventing tampering with contract content;
Support the upgrade of contract content under consensus;
Supports the writing of contract content into the book.

1.4 Encryption Security Technology

Asymmetrically encrypted public and private key pairs are used in the blockchain to build trust between nodes. The asymmetric encryption algorithm consists of a corresponding pair of unique keys (ie, a public key and a private key). Any person who knows the user's public key can encrypt the information with the user's public key and interact with the user to implement secure information. Because there is a dependency relationship between the public key and the private key, only the user holding the private key can decrypt the information. Any unauthorized user or even the sender of the information cannot decrypt the information.

The encryption function component has the following functions：

A) Supports international mainstream encryption algorithms, such as symmetric encryption algorithms such as AES256 and asymmetric encryption algorithms such as RSA and ECC；

B) Supports cryptographic algorithms, such as SM4 and SM7 symmetric encryption algorithms and SM2 and SM9 asymmetric encryption algorithms；

C) Should have a clear key management scheme to ensure the normal operation of the underlying blockchain security mechanism；

D) The encryption algorithm should have the ability to resist cracks, and it is advisable to regularly audit the security of the encryption algorithm. If necessary, use a higher encryption algorithm to break the computational complexity.

2. Overview

2.1 What is XCash

XCash is a brand new decentralized encrypted digital currency. It is a global open source public chain with the ability to deploy smart contracts.

XCash and its own smart contract carrier function together constitute the complete Turing.

Based on the concept of ETH and EOS, it has been reconstructed and has a decentralized blockchain payment network (thousands of TPS). It was previously mined by POW consensus and later through POW and XDPOS consensus mining. Based on XDPOS, It achieves smart contract separation, has a DPS Store of millions of TPS, and an efficient full-duplex gateway provides lightning-fast communication between the underlying payment network and the Dapp Store.

2.2 What is XHash

XHash is a mining algorithm used in the dawn stage after the XCash main chain goes online.

XCash generates new blocks by mining. Computers distributed all over the world compete for new block packing rights by computing XHash algorithm. Computers with optimal results obtain this package right after obtaining approval from the whole network, and package the whole package. The current transaction data of the network. At the same time, it obtains corresponding mining incentives and transaction package fee awards. The entire network generates a new block every 15 seconds on average.

The specific content of the algorithm is as follows:

1. There is a seed, each block can be calculated by block height up to that point.

2. From the seed, you can calculate a x MB pseudo-random cache for the light client storage cache.

3. From the cache, we can generate a 1 GB data set that indicates that each item in the data set depends on only a few items in the cache. The complete customer and miner store this data set. Data sets grow linearly with time.

Mining involves grabbing random slices of the data set and hashing them together. You can regenerate a specific part of the required data set by using the cache, so that the low-memory machine can perform validation because only the storage cache is required to verify.

The complete large data set is updated every y blocks, so most miners will work to read the data set instead of making changes.

2.3 What is Dapp Store and XDpos

Dapp Store is a brand-new concept. It is the carrier of smart contracts separated from the XCash main chain. The smart contract Dapp will all run in the Dapp Store, and the underlying network will focus on the decentralized blockchain payment in the future.

The Xdpos algorithm is a new algorithm that joins XHash in the new journey phase of the XCash main chain.

It is generated by Xdpos by election. The world produces 23 to 29 Dapp Store nodes after the election.

In the Xdpos consensus algorithm, the normal operation of the blockchain depends on the trustees (Delegates). These trustees are completely equivalent.

The duties of the trustee mainly include:

1. Provide a server node to ensure the normal operation of the node;

2. Node server collects transactions in the network;

3. The node validates the transaction and packages the transaction into blocks;

4. The node broadcasts the block and the other node adds the block to its own database after verification;

5. Lead and promote the development of blockchain projects;

The trustee's node server is equivalent to a miner in the Bitcoin network and can receive bonuses and transaction fees for the block while completing his or her own job.

The number of trustees for a blockchain project is determined by the project sponsor and is generally 101 trustees. Any one currency holder can participate in both the voting and the

campaign trustee.

Users can vote at any time and withdraw their votes. The weight of each user's vote is proportional to their own currency. Voting and ballot cancellations can be conducted at any time. After the round of elections are completed, the highest voter rating is 101 (generally 101, or other figures, as determined by the blockchain project owner). Each user becomes the project. Trustee, responsible for packaging blocks, maintaining the operation of the system and receiving appropriate rewards.

The fundamental purpose of the election is to vote out the 101 users who are most beneficial to the development and operation of the project in the community through the vote of everyone.

The 101 users' server nodes can not only maintain the efficient operation of the system, but also contribute their own ability to promote the development of the blockchain project.

In this way, the decentralized electoral consensus is achieved while ensuring the efficiency of the entire system and reducing energy waste.

2.4 Fundamental

XCash supports the operation of the entire decentralized network through POW and XDPOS consensus mining. The main network itself will provide complete smart contract deployment capabilities. Based on deployed smart contracts, users can arbitrarily design DApps to meet various needs. Release their own decentralized applications.

During the new journey, the smart contract will be migrated into XCash's newly designed Dapp Store, which can accommodate all kinds of decentralized applications and provide data circulation performance of millions of TPS.

XCash clients distributed all over the world voted for 23 to 29 Dapp Stores participating in the election through XDPOS rules. The underlying decentralized blockchain pure payment network exchanges data with the Dapp Store through the speed gateway.

XHash focuses on the underlying payment, Xdpos focuses on Dapp Store and its smart contracts.

Decentralized Tokens for Various Industries Based on XCash Distribution.

2.5 XCash's Vision

Become a global decentralized open source blockchain "Paypal", globalize cryptocurrency applications, and provide high-speed and efficient carrier for Dapp in various industries.

3.Technology Architecture

3.1 Technology Architecture

The purpose of XCash design is to integrate and enhance concepts based on scripts and original protocols, so that third-party service developers, merchants/users, and users can create any consensus-based, scalable, standardized, feature-complete, Easy to develop and coordinated application.

3.2 Underlying Technology

XCash uses Ethel's low-level technology to create an ultimate and abstract base layer - a blockchain built into the Turing Complete Programming Language. This allows anyone to create contracts and decentralize applications and set up their own freely defined Ownership rules, transaction methods and state transfer functions.

In the XCash system, the state consists of objects called "accounts" (each account is a 20-byte address) and a state transition group that transfers value and information between the two accounts. Similar to Ethereum, the XCash account contains four parts: a random number, a counter used to determine that each transaction can only be processed once; an account balance; the account's contract code (if any); and the account's storage (default Is empty).

3.3 Account Type

XCash will have two types of accounts: all external accounts (controlled by private keys) and contract accounts (controlled by contract codes). All external accounts have no code, and people can send messages from an external account by creating and signing a transaction. Whenever a contract account receives a message, the code inside the contract is activated, allowing it to read and write internal stores, send other messages, or create contracts.

3.4 ASD

XCash uses the P2P distributed signature system to ensure security. P2P networks are self-organizing, load-balanced, fault-tolerant, low-cost, and high-availability features. A P2P network made up of a large number of peer nodes can provide huge computing power while having a low cost. The project's distributed secure CA solution distributes digital signature calculations originally performed by high-performance servers to P2P networks.

3.5 Advantage

Code open source:
A stable decentralized global blockchain that is as difficult to destroy and man-made as Bitcoin.

Easy payment:
Decrypting digital funds in decentralized scenarios can also be quickly credited.

Security:
No information service provider can obtain user data, only wallet address, no personal information.

Easy to Develop:
Developers need only basic blockchain knowledge to deploy smart contracts on XCash, enabling decentralized applications with the desired functionality.

Token Support:

The XCash main chain supports token token issuance from various industries. Any developer can issue XCash-based ERC20 Token token features: security, ease of use, green, classification, scale, privacy, high frequency, free.

Extra features
● Multi-development language support: In the initial stage after the mainline is officially launched, the XCash team will continue to develop a third-party payment API library for the main chain. Once completed, it will provide a one-click access to the XCash payment API that is not limited to the following development languages: php, java, c#, c++, Objective c, go, ruby, python, lua, js. At any time around the world, simply run the XCash client and use third-party one-click API access to quickly, reliably, and securely XCash. Receipt payment function.

● Several exchanges cooperate: Before the official launch of the XCash main chain, the team will complete communication with several exchanges and technology docking to ensure that the XCash can be traded on the exchange immediately after the main chain is officially launched. After that, the team will continue to communicate with the exchanges. And provide complete technical support to ensure that XCash can be launched on more and more exchanges.

● Sustainable Development: Each year adds 1-2% of the new currency; compared to the current year where the majority of cryptocurrencies increase by 5% to 30% (ETH currently increases by 26% and EOS increases by 5% each year), the number of XCASH additions is much smaller. XCASH has more efficient transaction verification, excavator system, can save more than 60% of computing power or hundreds of millions of dollars in electricity in the future.

4、Roadmap

On May 28, 2018, the main network was turned on and the POW consensus mining was started. The related technical support for the construction of the mine pool was soon provided.

On May 31, 2018, pre-sale of private placement was initiated, with a total of approximately 1.2 billion pre-sales. It is expected that the pre-sale will end on the official website.

On July 10, 2018, the main network was officially launched, and the code was completely open source.

In July 2018, trading on the upper exchange.

Around July 10, 2020, the "New Journey" XDpos and Dapp Store were initially developed. Invite the community to participate in the "New Journey" Hard Fork upgrade when consensus is reached.

5、XCash Allocation

The pre-sale of this private placement will be formally opened on 00:00 on May 31, 2018 (GMT+8, Singapore time), and will be initiated together with a number of recommended agents. For details, see the official website and promotional materials.

1.5 billion pre-distribution, including 1.2 billion pre-sales of private placements, 50 million for early investors and investment returns, 50 million for marketing, 80 million foundation locks for one year, 120 million development teams and funds It will be issued every six years from the main line.

The encrypted digital assets raised by this private placement will be used for the future development of the "new journey" and the operation of the XCash Foundation.

6、Core Team

Development Team：

Owen Wilson, University of Ottawa Master, former Apple, Microsoft, senior geek programmer. In-depth research on blockchain technology and industry chain since 2012. Very familiar with BitShares and EOS implementation mechanisms, technology lines, optimization programs.

Dee Kan, Hongkong University Computer Master, years of rich experience in software development, one of the early development contributors to ethereum, very familiar with the entire architecture of ethereum.

Edison Lee, University of British Columbia, Master of Computer Science, Senior Programmer, formerly Google, started researching blockchain technology years ago. Technical experts in smart contracts, public chains, cross-chains, exchange security, etc..

Yuko Ono, Nagoya UniversityMaster of Finance, has profound research and achievements in the field of economics and finance in the field of digital cryptocurrency.

Frank Pai, Nanyang Technological University, Master's degree, with deep accumulation in the field of big data mining, distributed storage, etc., participates in the research and development of multiple blockchain projects, and has 3 invention patents.

Advisory Team：

1. Eden Don, Massachusetts Institute of Technology, Ph.D. Senior research scholar in the field of decentralized blockchain. He has published cryptocurrency and blockchain related papers in many world-renowned academic journals.

2. Hedy Ye, The Hong Kong University of Science and Technology, M.Sc., a professional research fellow in the field of insurance and blockchain assets, was a former Prudential Corporation.

3. Kobs Kao, Computer major of a well-known University, Senior programmer. Has many years of full-time work experience in computer software programming. In-depth research and

practice of encryption algorithms, blockchain domain programming, Go language, ethereum source code senior researcher, has participated in multiple blockchain related projects in github , and contribute a lot of open source code.

7、Risk Warning

Systematic Risk：

It refers to the possible changes in the returns due to global common factors that affect the returns of all securities in the same way. For example, policy risks - At present, the regulatory policies of various countries for blockchain projects and private equity pre-sale financing are not yet clear. There is a certain possibility of loss of participants due to policy reasons; if market risk, the overall value of the digital asset market Being overvalued, then the risk of investment will increase. Participants may expect the growth of private pre-sales projects to be too high, but these high expectations may not be realized. At the same time, systemic risks include a series of force majeure factors, including but not limited to natural disasters, large-scale computer network failures worldwide, political turmoil, etc。

Monitoring the Risk of Absence：

The transaction of digital assets including XCash has extremely high uncertainty. Due to the lack of strong supervision in the field of digital asset trading, there is a risk that electronic tokens will surge and plunge and be controlled by the dealer. Individual participants will enter the market if they are in the market. Lack of experience may make it difficult to resist the asset shocks and psychological pressure brought about by market instability. Although scholars, experts, media, etc., sometimes give suggestions for careful participation, there is no documented regulatory method and clause. Therefore, it is difficult to effectively avoid such risks at present.

Regulatory Risk：

It is undeniable that in the foreseeable future, regulatory regulations will be introduced to restrict the regulatory blockchain and electronic token fields. If regulators regulate the field, the tokens purchased during the private pre-sale period may be affected, including but not limited to fluctuations or restrictions in price and e-commerce.

Inter-team Risk：

Currently, there are many teams and projects in the field of blockchain technology. The competition is fierce and there is strong market competition and project operating pressure. Whether the XCash project can break through many outstanding projects and is widely recognized is not only linked to its own team ability and vision planning, but also affected by many competitors and even oligarchs in the market, and there is the possibility of vicious

competition.

In-team Risk：

XCash brings together a team of talents with both vitality and strength, attracting senior practitioners in the blockchain field and experienced technical developers. As a pioneer in the global blockchain technology field, the stability and cohesiveness within the team are critical to the overall development of XCash. In the future development, it is not ruled out that there is a possibility that the core personnel will leave and the team internal conflicts will cause the XCash to be negatively affected as a whole.

Project Co-ordination and Marketing Risk：

The XCash founding team will spare no efforts to achieve the development goals set out in the white paper and extend the project's growth potential. At present, XCash has a relatively mature business model analysis. However, due to the unpredictable factors in the overall development trend of the industry, the existing business model and co-ordinating ideas are not in good agreement with the market demand, which results in unacceptable profitability. At the same time, as this paper may be adjusted as the project details are updated, if the details of the project update are not timely obtained by the private placement participants, or the public is not aware of the latest progress of the project, the information asymmetry between the participants or the public The lack of awareness of the project affects the subsequent development of the project.

Project Technology Risk：

First, the project is based on cryptographic algorithms. The rapid development of cryptography will inevitably bring potential risks. Second, technologies such as blockchain, distributed ledger, decentralization, and disagreement with falsification support core business development. The XCash team cannot fully guarantee the landing of the technology; again, during the process of project update and adjustment, it may find that there are loopholes that can be remedied by issuing patches, but it cannot guarantee the extent of the impact of the loopholes.

Hacking and Criminal Risk：

In terms of security, the amount of individual supporters is small, but the total number of people is large, which also puts forward high requirements for project security. Electronic tokens are characterized by anonymity and hard-to-retrospectiveness, which are easily exploited by criminals, or attacked by hackers, or may involve criminal activities such as the transfer of illegal assets.

Other Risks not currently known：

With the continuous development of blockchain technology and the overall trend of the industry, XCash may face some unanticipated risks. Participants are asked to fully understand the team background before they participate in decision-making, to know the overall framework and ideas of the project, to rationally adjust their vision, and to participate in the token crowdfunding program.

Disclaimer

This document is for information purposes only. The contents of the document are for reference only and do not constitute any investment advice, advice or invitation for the sale of stocks or securities in XCash and its related companies.

Such invitations must be made in the form of a confidential memorandum and must comply with the relevant securities laws and other laws.

The contents of this document must not be construed as forcing private placement. Nothing related to this White Paper should be deemed to be involved in private pre-sales, including requesting a copy of this white paper or sharing this white paper with others.

Participating in private equity pre-sale represents that the participant has reached the age standard and has full civil capacity. The contract with XCash is real and effective.

All participants volunteered to sign contracts, and XCash made a clear and necessary understanding before signing the contract.

The XCash team will continue to make reasonable attempts to ensure that the information in this white paper is true and accurate. During the development process, the platform may be updated, including but not limited to platform mechanisms, tokens and their mechanisms, and the distribution of tokens. Some of the contents of the document may be adjusted in the new white paper as the project progresses. The team will publish the updated content by posting an announcement or a new white paper on the website. Participants are requested to obtain the latest version of the white paper in time, and adjust their own decisions in a timely manner based on the updated content.

XCash expressly stated that it does not assume any loss caused by the participant's reliance on the content of this document, the inaccuracy of the information in this document, and any actions resulting from this document.

The team will spare no effort to achieve the goals mentioned in the document. However, based on the existence of force majeure, the team cannot completely fulfill its commitment.

XCash, the official token of XCash, is an important tool for platform performance and is not an investment product.

Owning XCash does not grant ownership, control, or decision-making rights to its owner's (XCash) platform.

XCash as an encrypted token used in XCash does not fall into the following categories：

(a)Any kind of currency；

(b)Securities；

(c)Entity of legal entity；

(d)Stocks, bonds, notes, warrants, certificates, or other instruments that grant any rights.

The value-added of XCash depends on the laws of the market and the requirements after the application is made. It may not have any value. The team does not make any commitment to its value-added, and is not responsible for the consequences of its increase or decrease in value. To the fullest extent permitted by applicable law, the damages and risks arising from participating in crowdfunding, including but not limited to direct or indirect personal damages, loss of

commercial profits, loss of business information or any other economic loss, the team does not Take responsibility.

The XCash platform complies with any regulatory regulations and industry self-regulations that are conducive to the healthy development of the private equity pre-sale industry. Participant participation means that the representative will fully accept and observe such inspections.

At the same time, participants disclosed that all information used to complete such inspections must be complete and accurate.

The XCash platform clearly communicated possible risks to participants. Once participants participate in private equity pre-sale crowdfunding, they have confirmed their understanding and endorsement of the terms and conditions in the detailed rules, and accept the potential risks of the platform at their own risk.

The XCash team and the XCash Foundation have the final interpretation right of the above explanation. All the terms apply to Singapore law and ultimately belong to Singapore administrative jurisdiction.

（Note: According to the current laws and regulations, KYC certification and follow-up private placement services for citizens in the following countries and regions are temporarily unavailable: China (Mainland), United States (Overall), Canada, Singapore. ）