ETHEREUM GOLD

ETG

GOLDEN PAPER

SPECIFICATION

This document is Ethereum Gold Technology Golden Paper version V3.5. It mainly introduces the background, positioning, technical characteristics and application scenarios of ETG. In the future, we will continually upgrade this document to keep it consistent with new technology evolvement. For the latest and more information of ETG, such as technical Golden papers, software releases, developer communities, and more, please visit the official site: https://etgproject.org .

CONTACT US

Golden Paper: goldenpaper@etgproject.org
Developer dev@etgproject.org

DISCLAIMER

AS Blockchain technology progresses, the ETG team will improve and refine existing technology solutions as needed, and continue to improve the technical golden paper.

ABSTRACT

Blockchain technology is considered to be the fifth most likely technology which will lead to disruptive revolution in productivity and production relations, following the steam engine, power, information technology and Internet. Since creation of Blockchain technology represented by Bitcoin in 2009, this technology has made great progress and received more and more attention. Especially in recent years, Blockchain technology has become global focus. From core technologies to chain applications, comprehensive explorations have been carried out for Blockchain. However, as far as current Blockchain technology is concerned, there is a big gap between chain technology and various applications. Especially, there are many technical difficulties around Blockchain core technologies, which need breakthrough. At present, the infrastructure to support development of Blockchain applications is unstable, thus many applications are not effective. Therefore, it is urgent to make research and development on Blockchain infrastructure, thus providing reliable support for various Blockchain applications, as well as promoting implementation of Blockchain applications in all kinds of industries, which makes Blockchain serve human beings faster and better. We propose an infrastructure for global value-internet, ETGP. It aims to solve the problems such as low applicability, transaction congestion, high commissions, long confirmation latency, weak resistance to quantum attacks, poor anonymity in communication and transaction, incapability in crossing and merging chains, large space for storage etc.

ETG would optimize and improve Blockchain technology in all aspects including protocols and mechanisms, and become a genuine infrastructure of Blockchain 4.0. Also, ETG would provide a platform for developing various apps (distributed Apps), as well as feasible solutions to construct a global value-internet. ETG focuses on core technology of Blockchain infrastructure and platform. Our goal is to build an infrastructure conquering current key technical problems and supporting all domain applications in terms of ecological view. Main technological innovation of ETG includes: (1) Underlying P2P network, combining the advantages of Tor-based anonymity and Blockchain-based distributed VPN, we design a novel anonymous P2P overlay network, including anonymous access method and encrypted communication protocol, which greatly enhances anonymity of nodes in the network and ensures that it's hard to trace node address and to crack communication protocol. (2) Data structure, a new data structure HashNet derived from DAG (directed acyclic graph) is proposed, which greatly reduces storage space required by nodes and improves efficiency and security of data storage. (3) Consensus, we design an efficient and secure double-layer consensus mechanism consisting of HashNet consensus and BA-VRF (Byzantine Agreement based on Verifiable Random Function) consensus, which supports high transaction concurrency, fast confirmation and building eco-systems for different application scenarios. In version 1.0, due to the fact that HashNet consensus is much difficult to implement, we First implement a double-layer consensus mechanism combining DAG consensus with BA-VRF.

Anti-quantum attack, new antiquantum algorithms are devised, which replaces existing SHA series algorithm with the Keccak-512 hash algorithm, and replaces ECDSA signature algorithm with an integer lattice-based NTRU sign signature algorithm. These algorithms reduce the threat coming from development of quantum computing and gradual popularization of quantum computer. (5) Transaction anonymity, based on anonymity characteristics of cryptocurrency such as Monero and ZCash, one-time key and ring signature are applied to transaction anonymity and privacy protection, which performs with high cost-effective ratio and excellent security. As a function of choice, zeroknowledge proofs are used to satisfy privacy requirements in different application scenarios. (6) Smart contracts, we design Moses virtual machine (MVM) which supports declarative non-Turing complete contract as well as advanced Turing complete contract programmed in Moses language. MVM is able to access Blockchain data conveniently and securely, and supports issuance of third-party assets, which can be integrated into applications in terms of public, permissioned (private) or consortium (hybrid) Blockchain. (7) Crossing and merging chains, we adopt chain-relaying technology to solve the problems in crossing chains transaction and transparent operations among multiple chains, which not only can maintain independence of crossing chains operation, but also reuses various functions of ETGP. (8) Ecological motivation, various token allocation methods are used, which support double-layer mining for incentives.

(9) Industrial application, we design lots of industrial common interfaces in form of JSON-RPC, satisfying different scenarios such as circulation payment, data transmission, data search and contract invocation. ETG supports implementation for a variety of applications including anonymous communications, power sharing, storage sharing, bandwidth sharing, reputation sharing (credit guarantee), and it provides open interfaces for third-party app development. By connecting with various application scenarios, ETG can cooperate with kinds of service providers and application providers to support commercial organizations or government agencies to build public, consortium or permissioned chain application systems according to business characteristics and requirements. ETG will reform existing operational mode in Internet. It introduced Token distribution mechanism for incentive to inspire community to maintain ETG public chain and to develop apps. ETG will stimulate more value and network spreading effects on public chain, and turn economic incentive system into a self-renewing system, and create a completely decentralized ecosystem of value internet and value transfer.

Background 1.1. Blockchain Development Overview

Blockchain can be used as a peer-to-peer (P2P) decentralized system to store the pseudonymous transaction records in a trustless environment. Blockchain is the core technology of Bitcoin which was First proposed in 2008 and was implemented in 2009.

Blockchain is essentially a distributed ledger, in which all committed transactions are stored in a chain. This chain continuously grows when the new transactions have been confirmed. Blockchain is one of the most popular topics nowadays. First of all, it is a kind of social thought, which indicates the coming of a new era of transformation and change of human society. Kelly in the book "Out Of Control" describes: the natural, social, and technological evolution of biological logic is from the edge to the center then to the edge, from out of control to being controlled then to out of control. The technology base of Blockchain is distributed network architecture, because of the maturity of distributed network technology, it is possible to establish the business structure effectively by going to center, weak center, sub center and sharing, consensus and shared organization structure. Today's Blockchain technology has undergone several iterations: (1) Blockchain 1.0: Cryptocurrency. In early 2009, the Bitcoin network was officially launched. As a virtual currency system, the total amount of bitcoin is defined by network consensus protocol. No individual or institution can freely modify the supply and transaction records therein. The underlying technology of Bitcoin, the Blockchain, is actually an extremely ingenious distributed shared ledger and peer-to-peer value transfer technology that has the potential to affect as much as the invention of double entry bookkeeping. (2) Blockchain 2.0: Smart contracts. Around 2014, industry community began to recognize the importance of Blockchain technology, and create a common technology platform to provide developers with BaaS (Blockchain as a service),

which greatly improve the transaction speed, reduce resource consumption and support multiple consensus algorithms such as PoW, PoS and DPoS, as well as making app development easier. (3) Blockchain 3.0: Blockchain technology application. After 2015, with the rise of Blockchain 3.0 technology based on DAG data structures, such as Byteball and IOTA, Blockchain systems are more efficient, scalable, highly interoperable, and offer a better user –3– experience than before. Applications of Blockchain gradually extend to healthcare, IP copyright, education, and IOT. Broader applications such as sharing economy, communications, social management, charity, culture and entertainment. (4) Blockchain 4.0: Blockchain ecosystem. Recently, Blockchain 4.0 technology based on Hashgraph data structure has gradually attracted attention of industry community. The consensus algorithm based on Hashgraph can achieve a qualitative growth in transaction throughput and scalability. The Blockchain will become the infrastructure of industry and form a consolidate ecosystem, which also changes people's lifestyle extensively and pr

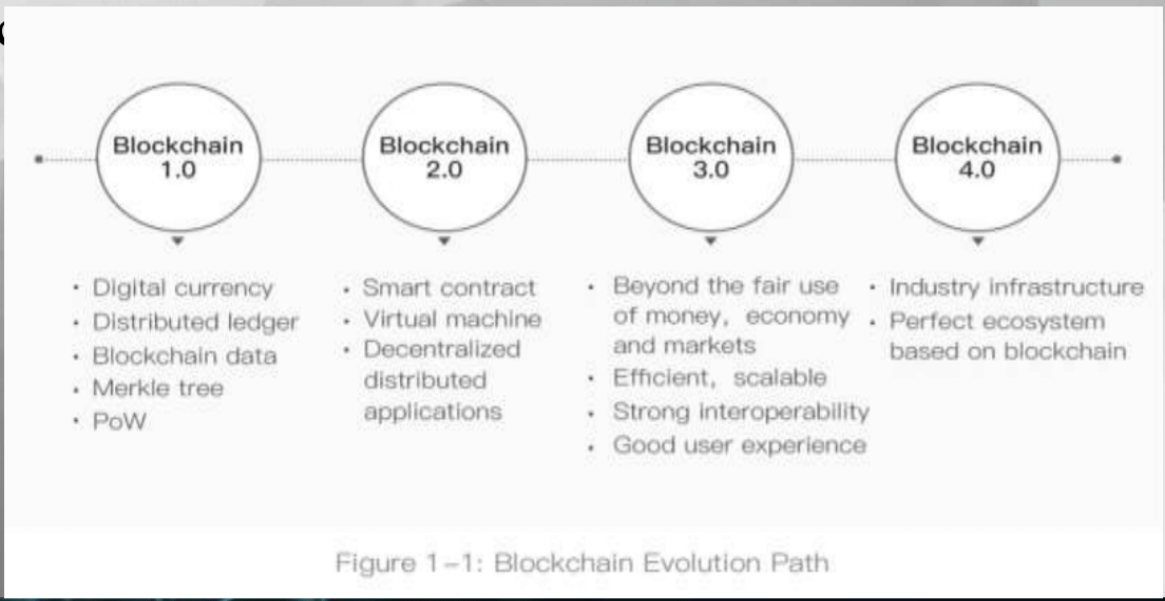


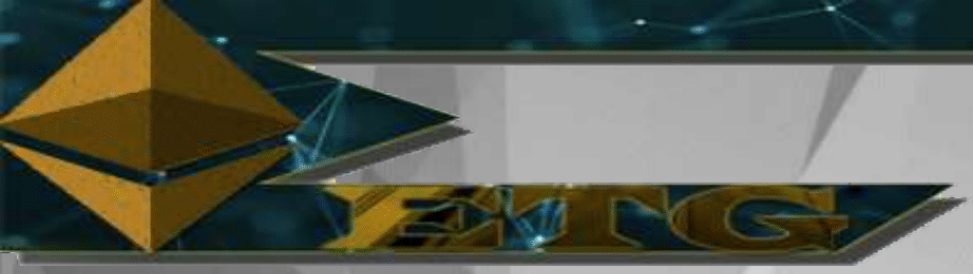
Figure 1–1: Blockchain Evolution Path

In recent two years, although some countries are conservative about use and development of cryptocurrencies, underlying technologies and applications of Blockchains are paid much attention by the entire world. With the deepening of recognition of Blockchain technology and application domain, people show great enthusiasm in development and implementation of Blockchain core technologies and chain applications. The research and exploration on Blockchain technology mainly focus on three aspects: (1) underlying technology and infrastructure layer: it mainly contains the basic protocol and related hardware. (2) General application and technology extension layer: it provides services, interfaces and related technical exports, including smart contract, quick calculation, mining service, information security, data service, BaaS, solution, traceable anti-counterfeiting and etc., for vertical industries. (3) Vertical industrial application layer: Blockchain is implemented in vertical areas such as Finance, digital currency, entertainment, supply chain, healthcare, law, energy, public welfare, social, Internet of Things and agriculture. At present, people invest a great deal of enthusiasm in development and application of Blockchain technology. Among the teams engaged in Blockchain research and development, proportion of teams engaged in underlying technology research is about 20%, and proportion of teams using chains for application scenarios and vertical industries is 80%. Compared with application layer, underlying technologies can create token market value. In addition, it changes the traditional Internet-centric mode, i.e., data are centralized at application layer.

Under Blockchain system, application layer becomes a complete service provider, it no longer owns user trade and data value. These personal data are distributed to users, and underlying technologies is more valuable than application layer.

BLOCKCHAIN PROBLEMS:

Current Problems of Blockchains Currently, various Blockchains such as EOS, NEO, ArcBlock and other projects emerge continuously, but most of them are based on Ethereum. They are far from criteria of Blockchain 4.0. Most of project teams which implement Blockchain with application scenario are limited by performance, applicability and stability of underlying chain. And they are currently at an early stage. Although it is estimated that many industry applications may rise in 2018, with the underlying agreements are constantly changing, more than 98% of the projects will be eliminated by history. The current Blockchain technology mainly has the following problems. Poor performance. Performance is one of main challenges for current Blockchain technology. Bitcoin is designed to handle only seven transactions per second, and Ethereum can only handle a few more. As of December of 2017, a simple CryptoKitties application can slow down Ethereum and increase transaction fees dramatically. Today's consumer applications must be able to handle tens of millions of active users daily. In addition, some applications will only become valuable when certain throughput is reached. The platform itself must be able to handle a large number of concurrent users.



A Fine experience demands reliable feedback within only second-class delays. Long latency frustrates users and make applications built on Blockchains less competitive with existing non-Blockchain alternatives. Difficult to use. Today's Blockchain applications are built for the few tech whizzes who know how to use them, rather than common users. Nearly all Blockchain applications require users to either run a Blockchain node or install a "light node". It takes a long time for users to adapt to application. For example, while the Ethereum-based game CryptoKitties is probably the most user-friendly decentralized App ever built, it still requires users to install the Metamask light wallet browser extension. Users also need to know how to buy Ethers securely and use them with Metamask. To attract large numbers of people, Blockchain applications need to be as simple as today's Internet and mobile apps. Blockchain technology should be completely transparent to the consumer. High cost. The extremely high cost of using Blockchain technology is a major barrier to adoption. It also limits developers who need the flexibility to build free services. Just like today's Internet and mobile Apps, there is no need to pay every operation during Blockchain transaction. Similar to the Internet, Blockchain technology should be able to support free applications. Making Blockchain free to use is key to its widespread adoption. A free platform will also empower developers and businesses to create valuable new services they can monetize, rather than having users pay fees to use the Blockchain network. Platform lock-in. Same as the early days of any computing technology, Blockchains have critical "platform lock-in" problems

Developers have to decide which Blockchain to develop, then implement platform-specific code, which makes it very difficult to switch an application to another Blockchain. Developers don't want to be locked into working with a certain Blockchain technology. They need freedom to evaluate, use, and switch between options. Some applications may even need to run on multiple platforms to provide best user experience. Low applicability. People have high expectations for Blockchain, kinds of media paint a bright future for decentralized applications for the public, especially with the increasingly high prices of cryptocurrencies. In reality, however, Blockchain technology is still in its infant stage. Most Blockchain services lack rich features and don't have a mechanism to encourage the community to contribute to the feature stacks. Therefore, there is an urgent need to study the underlying mechanism of Blockchain, and redesign or improve the various key technologies of Blockchain to solve the problems such as transaction congestion, high transaction fees, long confirmation latency, weak anti-quantum attack capability, low anonymity of communication and transaction, weak crossing and merging chain capability, large storage space etc. We aim to implement a real practical support mechanism for all levels of value transfer network, provide the infrastructure for all kinds of value transfer applications, and a underlying development platform for all kinds of apps and practical and feasible solutions for constructing the global value transfer and value interne

SMART CONTRACT

Blockchain technology brings us a system with decentralization, no trust, no falsification, and high reliability. In this environment, the smart contracts are of great potential. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible. Smart contract needs to Find a subtle balance between the safety and usability. Existing blockchains are mostly of a monotonous design, seeking for the balance between safety and usability under the restriction of a given type of smart contract, and usually cannot guarantee rich user experience and satisfy various trading demands. The transaction script of the Bitcoin blockchain is an early prototype of the smart contract. It is Turing-incomplete, with low complexity and light weighted. For the past ten years of the Bitcoin, its transaction script has never experience any safety compromise. However, the Bitcoin transaction script has a highly limited function, and can only be used for payment verification. The Ethereum blockchain supports a Turing-complete smart contract which is programmed in Solidity. It enriches the functionality of the smart contract and largely extends the application scenarios for the blockchain.

Unfortunately, an Ethereum smart contract suffers from potential safety hazards. The DAO incident is a famous example that the safety problem in the Ethereum smart contract leads to the split of the community. Built upon the smart contract and the Moses Virtual Machine (MVM), Inter Value takes a similar idea as the hierarchical design of the computer storage system and supports both the Declarative Turing-incomplete smart contract and the Advanced Turing-complete smart contract. The users choose between the two kinds of smart contracts based on their experience and trade demands, hence achieve the balance between the safety, functionality, complexity and cost. The declarative contract is easy to deploy, with a high level of safety and close to legal contract statements. The advanced contract is more difficult to deploy, and mostly used for –43– developing the app with a logic of higher complexity. The two smart contracts have different charging schemes. The declarative contract charges according to the number of bytes being taken, while the advanced contract charges according to the number of ETG tokens being consumed.

MOTIVATION:

ETG Pay Service

Vision: decentralize payment companies , we built ETG project to make transactions between companies & communities very easier depending on Ethereum blockchain.

Future steps :

USD-G or USD GOLD will be our stable token in the near future , we are developing a new contract for USD-G based on mintable / burned tokens ,