TrueChain

Whitepaper

TrueChain

Contents

TrueChain is decentralizing global asset transactions.

Background
The Rise of Global Digital Asset Transactions

Over the past 3 years, there have been a number of public blockchains. Each of these blockchains adopts a certain kind of consensus. All wanted to solve the impossible triangle problem and achieve efficiency, decentralization, security in the same time.

A public chain that truly solves the impossible triangle problem could ultimately support potential large volume of transactions of digital assets worldwide in a decentralized financial infrastructure that is totally independent of centralized authorities and centralized trust.

There are three trends that we pay most attention to:

A. The liquidation of digital assets on blockchain

B. The tokenization and liquidation of all financial assets and real estate assets on blockchain

C. Enterprise applications on blockchain

These trends are providing real values to public blockchains after the fall of utility tokens.

Therefore, we need a public chain to have following features:

A. Permissionless

B. Efficient, or fast

C. Secure

D. Decentralized

E Right gas model to incentivize miner communities and token holder communities

TrueChain is building up such a public blockchain and the ecosystem around it. This whitepaper will brief consensus, architecture, incentive

model, and TrueChain ecosystem. There are more details available on Web. For technical details, there is a yellow paper at https://arxiv.org/abs/1805.01457. For public chain developers, the GitHub link is https://github.com/truechain.

TrueChain's Consensus and Technology
Minerva Hybrid Consensus

After the invention of smart contract mechanism by Ethereum, there has been a continuous evolution of consensus technologies. The first stage was to improve efficiency of blockchain networks by adopting protocols that use delegation to reduce processing nodes. Among these technologies, DPoS was the most successful and mostly adopted. However, there is a fatal problem of DPoS chains -- the inability to support decentralized trust ultimately, and the inevitable fate to be reduced to a centralized infrastructure.

There are a number of trials to invent consensus technologies that could solve the impossible triangle:

> **A. Casper is a roadmap that eventually transforms ethereum into a PoS public chain**
>
> **B. DAGs are consensus mechanisms that allow parallel processing of transactions normally on a PoW chain**
>
> **C. Hybrid Consensus is a way to allow a BFT protocol to work in a permissionless environment**
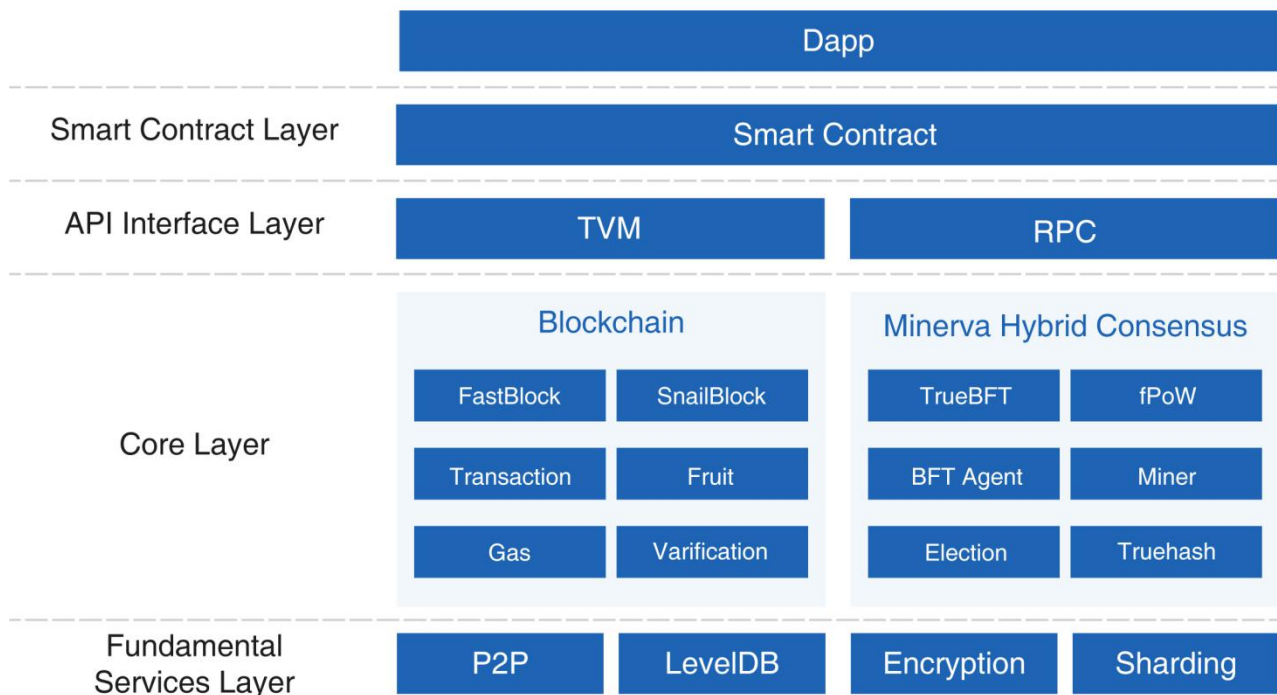
TrueChain adopts its own version of hybrid consensus.

Hybrid consensus was firstly proposed on a research paper (https://eprint.iacr.org/2016/917.pdf) as a theory. TrueChain's core research team and core engineering team largely improved the original proposal and delivered the first working implementation. There are few key features of Minerva Consensus:

> **A. Replaced Nakamoto PoW (traditional PoW protocol) with fPoW**
>
> **B. Designed TrueHash, a fundamentally ASIC-resistant algorithm**
>
> **C. Designed a working architecture of DPoS-fPoW consensus protocol**

The fPoW protocol eliminates selfish mining attack (a.k.a 25% attack) and brings miners of different hash powers to the miner community. TrueHash makes ASIC mining hard. The DPoS-fPoW hybrid consensus achieves speed, decentralization and security.

The architecture of TrueChain is as below.

TrueChain Blockchain Technology Architecture

	Dapp	
Smart Contract Layer	**Smart Contract**	
API Interface Layer	**TVM**	**RPC**
Core Layer	**Blockchain**	**Minerva Hybrid Consensus**
	FastBlock / SnailBlock / Transaction / Fruit / Gas / Varification	TrueBFT / fPoW / BFT Agent / Miner / Election / Truehash
Fundamental Services Layer	P2P / LevelDB	Encryption / Sharding

TrueChain is implemented as a double-chain structure (Fast Chain and Snail Chain).
The block of Fast Chain, which mainly contains the transactions and smart contracts, is generated by the BFT committee when they reach a consensus. Similar to Ethereum block, fast block provides TxHash, Root, ReceiptHash for other non-members to verify transactions included at fast block body.

The block of Snail Chain contains several fruits, and each fruit stamps the corresponding fast block. Fruit is hanged on snail block, when a fruit points to a fast block, the fruit stamps the fast block's hash and number in it. Every fast block has only one fruit to stamp its hash and number.

TrueBFT is PBFT implemention of truechain. The classical PBFT assumes less than ⅓ of the participating nodes are corrupt. TrueBFT assumes mildly adaptive adversary model to improve the chain quality.

The committee instance is switched after a fixed period of time (with the snail chain as a logical clock). The members of the next committee are chosen from Fruit and Block Miners of the current committee.

Truehash is the mining algorithm for TrueChain and is a fundamentally achieving ASIC resistant algorithm.The implementation of truehash is to set a group which is complex enough. The principle of truehash's switching algorithm is that the group elements will be changed every 12 thousand snail blocks and composed by these snail blocks. Because the hash value of the block is unpredictable in advance, it's impossible for anyone to know anything about the new algorithm. From the last cycle, to the algorithm being invalidated, there is only 88 days in total, so it makes no sense to produce ASIC in such a short period of time.

Incentive Model

The Ethereum block incentive model and gas model have been widely adopted for a long time in many public chains' designs. Over the year 2018, utility tokens have been largely failing because most of them are not backed by valuable assets. In other words, the value of utility tokens are unsure and their economic models are generally not successful. For example, a utility token with only economic model but no revenue would fail miserably.

Therefore, public chains have to support such asset backed tokens. The key to this problem is incentive model. The economic model of ETH has to be re-thought and a new incentive model has to be proposed to fulfill the needs of valuable transactions.

There is a recent article from TrueChain's research community stating the problem of Ethereum incentivization mechanism. https://www.reddit.com/r/ethereum/comments/arsu33/on_the_security_economics_of_public_blockchains/

An proper model has to incentivize more hash power with larger on- chain asset value in order to provide corresponding level of security to the network. Therefore such an incentive mechanism has to build a linkage between TRUE token and the gross value of assets being liquidated on TrueChain.

TrueChain is planning to implement three mechanisms. Combined they form the new incentive model.

Governance

TrueChain's goal of governance is to ultimately establish a decentralized governing model. At the time TrueChain was founded, it was contributed mostly by the founding time. In summer of 2018, TrueChain Foundation currently established a board of directors (7 people). Each of the seven directors is in charge of one part of the foundation's governance -- research, core engineering, product development, developers community & human resource, global token holders community, marketing and ecosystem building. Together the board directors make strategic and managerial decisions.

Given the blockchain industry's fast pace, the foundation's board is serving two purposes:

A. Risk control of the decision making process

B. Encourage thorough understanding of problems and improve decision quality

There is an elected president for the board of directors. The president's most important responsibility is to coordinate between each part of the foundation's work and guarantee that TrueChain's strategies and plans are well executed. This president is acting as an effective "CEO" of the project, but is re-elected every 3-6 months.

This governance model will last until TrueChain's mainnet is supporting a fairly large amount of tokenized assets on-chain and TRUE tokens are greatly distributed across large number of holders worldwide. After that, TrueChain will enter the era of totally decentralized governance. Under a decentralized governance model, TrueChain will form a Committee of Representatives that is elected by all TRUE holders, and a president will be elected from the Committee of Representatives by all TRUE holders.

A term limit will be imposed on both the committee and the president, with enforcement of smart contracts on TrueChain that transfers the rights of using Foundation funds to the newly elected committee.

Ecosystem

Global Developer Community & Dapp Development Support

There are over 3000 developers in TRUE tech community. The majority of them are from China, America, India, Singapore, and Vietnam.

TrueChain Developer Platform

TrueChain's in-house product team has built a developers' platform to support deployment and management of smart contracts. To access is, go to link http://dev.truechain.pro/

TrueGlobal Competitions

TrueGlobal is an on-going, independent community effort to support Dapp developments on TrueChain across the world. The first round of TrueGlobal competition has finished in Jan 2019 with more than 20 Dapps submitted to TrueChain's BetaNet.

TRUE Holder Communities

Over one year, there has been more than 280,000 TRUE holders worldwide. Active communities are located in East Asia, South-East Asia, Mid-East, North America and Europe. TrueChain has built up a network of community nodes (a.k.a. contributors) in each country.

Tools and Dapps

Blockchain browsers: TrueScan
Games: Candy Jungle,TrueCard, Red Packet;
Layer 2: Wallet: True Wallet ,Web wallet
Tokenization: TrueST(PandaST);

To be continued

Cross-Chain Protocol

Cross-chain features are mostly needed when an asset is to be issued on multiple chains. It is not as much important to exchange in a barter-economy manner across different public chains.

TrueChain's new TrueBridge： Support multi-resource cross-chain including digital assets, support unlimited cross-chain, to achieve a lightweight cross-chain solution through synchronizing a small part of the total block header chain.

Roadmap

Genesis Phase

September 2017 - October 2018

- ✓ TrueChain's white paper v1.0 released
- ✓ TrueChain technical yellow paper v1.0 released
- ✓ Hybird consensus mechanism design completed
- ✓ Stellar - - smart contract management engine — released and open sourced
- ✓ TrueChain's engineering roadmap released on github
- ✓ TrueChain Light Wallet released
- ✓ TrueChain's election system for decentralized nodes released
- ✓ TrueChain has been listed on OKex,ZB,BitThumb,HitBTC and many other major exchanges
- ✓ Globally TrueChain's token holder exceeds 100k
- ✓ Hybrid consensus framework code open source
- ✓ Hybrid consensus incentives release
- ✓ TrueChain technical yellow paper v2.0 released
- ✓ TrueChain TestNet — BetaNet released
- ✓ TrueChain's First Blockchain Explorer TrueScan launched
- ✓ Developer platform released
- ✓ > 10 Dapps running and testing on TrueChain BetaNet

Columbus

Late 2018 - 2020

- ✔ **Design PandaST Protocol**

- ✔ **Implement 3rd-party gas payment agent and reform gas fee mechanism**

- ✔ **Main Net Launch**

- ✔ **Reform public chain incentive model**

- ✔ **Increase and stabilize mining hash power for main net**

- ✔ **More Dapps & asset tokens on TrueChain**

- ✔ **More TRUE token holders globally**

- ✔ **More tokenized assets issued on TrueChain**

- ✔ **Growth of TRUE mining community**

- ✔ **More layer-2 infrastructures connected to TrueChain**

- ✔ **TrueChain listed on Binance Dex**

The Republic

2020 Onwards

- ✓ **Upgrade hybrid consensus to fpow + dpos**

- ✓ **Dpos Committee node campaign**

- ✓ **True Staking**

- ○ Truebridge upgrades and restructures

- ○ Truescan overall upgrade and reconfiguration

- ○ TPS upgrade to 10000

- ○ More Dapps & Asset tokens on TrueChain

- ○ More Tokenized Assets Issued on TrueChain

- ○ Truevm adds virtual machine based on wasm

- ○ Implement chain-to-chain interoperation protocol for TrueBridge

- ○ Support zero-knowledge proof and related privacy computation layer2

- ○ Growth of TRUE Holders Globally

- ○ Decentralized governance

The Future (from 2020.12-)

Milestone 1 : 2020.12-2021.3

part 1 of TrueChain 2.0

transaction parallel execution launch,tps will improve more

TrueChain bridge 2.0(gravity) update and launch

Truescan update,support all ecosystem and more functions

Milestone 2：2020.4-2021.6

part 2 of TrueChain 2.0

Consensus mechanism upgrade, will be upgraded from hybrid consensus

TrueChain 2.0 testnet launch

Milestone 3：2021.7-2021.9

TrueChain 2.0 official version launch

Node and wallet will also update with TrueChain 2.0

Milestone 4 : 2021.9-2022.2

TrueWallet update, support several popular public chains

Milestone 5: 2022.2-2022.12

TrueDAO starts
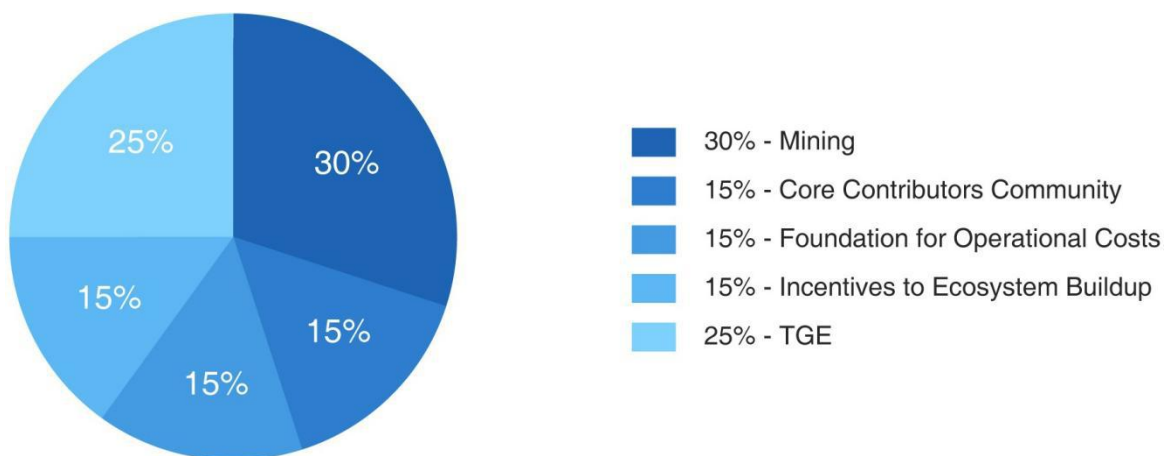
more eco projects will launch

Milestone 6: 2023.1-

TrueDAO update

Decentralized governance

Token Utilities and Token Distribution

TrueChain's mainnet currency is TRUE token, a utility token for transaction gas and staking. The total amount of issuance is 100 million TRUE tokens. The proportion of TRUE distribution is shown as follows:

30% - Mining
15% - Core Contributors Community
15% - Foundation for Operational Costs
15% - Incentives to Ecosystem Buildup
25% - TGE

TrueChain