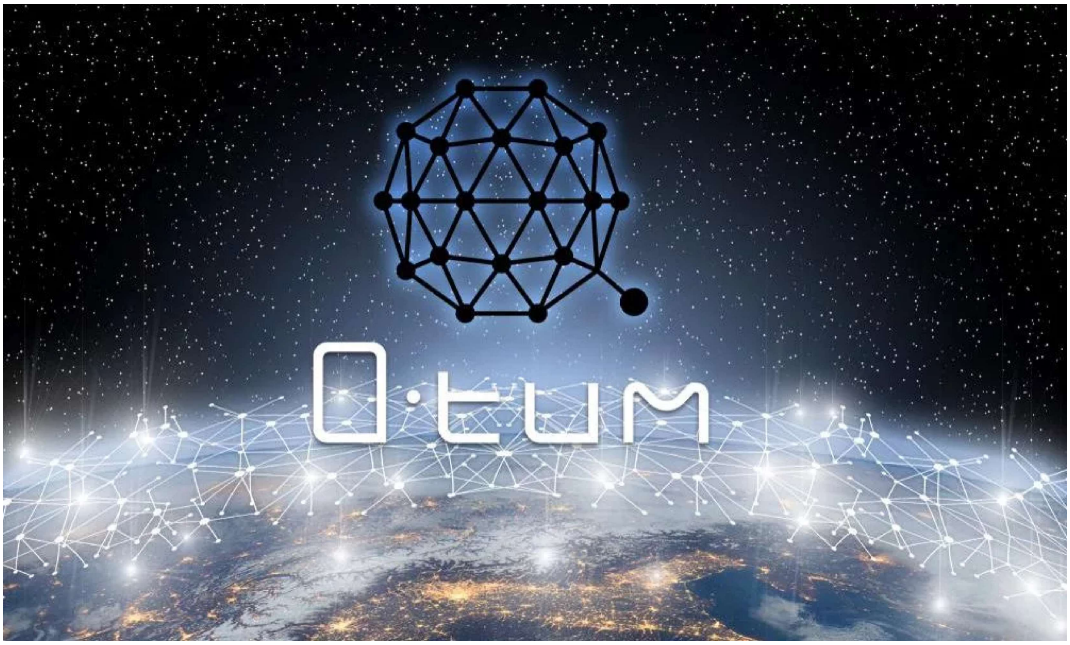
What is Qtum? The blockchain for business applications

By JAKE SIMMONS — May 15, 2019



What is Qtum?

Qtum (pronounced “Quantum”) is a Singapore-based blockchain platform designed to create a fully distributed smart contract platform and value transfer protocol. The idea behind the platform is to make smart contracts simpler and more secure, making the technology more accessible to industry and business applications. So the main goal is to build a bridge between the blockchain world and the “real world” in the form of industry. At the same time Qtum strives for interoperability with leading cryptocurrencies like Bitcoin and Ethereum, with which Qtum should be compatible.

- According to whitepaper and official website, Qtum has summarized the following goals:
- Manufacturing of a Bitcoin variant with Ethereum Virtual Machine (EVM) compatibility
- Creation of a blockchain for industrial and business applications
- Creation of use cases for mobile devices and thus adaptation of blockchain technology to the everyday life of Internet users
- Implementation of a completely decentralized Proof-of-Stake transaction validation
- Solution of the scalability problem of blockchains

Within the whitepaper of Qtum it also becomes clear with which other cryptocurrency Qtum wants to

- Proof-of-Work (PoW) transaction validation prevents scalability to the point where Ethereum cannot be used for real business applications.
- The safety of Ethereum is inadequate.
- Ethereum is unable to automate cross-company information logistics.
- There is a lack of a secure and stable virtual machine with proof-of-stake transaction validation.
- A formally verifiable Smart-Contract language is missing.
- Lite wallets for Smart Contracts, which do not require the download of the complete blockchain, are (currently) not possible.

Founded by Patrick Dai in March 2016, the project completed the **Initial Coin Offering (ICO)** in March 2017 and raised $15.6 million in 117 hours. QTUM's Mainnet went live a few months later, in mid-September 2017.

Mashup between Bitcoin and Ethereum

Qtum, is also often called a **mashup between Ethereum and Bitcoin** as it aims to combine the best of both crypto currencies. Specifically, Qtum uses the Unspent Transaction Output (UTXO) model, which also uses Bitcoin and intends to provide a smart contract platform like Ethereum at the same time.

One of the main reasons for this mashup is the goal to make the Qtum Blockchain also accessible for Light Clients (mobile devices). In the opinion of the Qtum developers, this is difficult to achieve with Ethereum technology. In contrast, Bitcoin's "Simple Payment Verification" (SPV) should be ideally suited for light clients.

Unspent Transaction Output (UTXO) Model

The core technology for the fusion of Ethereum and Bitcoin is the Account Abstraction Layer (AAL), which maps the **Bitcoin UTXO approach to Ethereum's account-based system**. But what exactly does the AAL do?

UTXO technology works in such a way that each transaction on the Bitcoin block chain is a reference to a previous transaction. In the event that the entire amount from the previous transaction is not spent (not sent to a new recipient), the unspent amount is sent back to the sender).

In contrast, Ethereum works like a traditional banking book, which does not track transactions but the balance of an account. Each transaction on the Ethereum block chain causes a change in the balance in the global ledger. The individual transactions are therefore less significant.

According to the Qtum team, the UTXO model (from Bitcoin) makes it easier to validate transactions, enabling greater transaction throughput. While Ethereum can currently handle about 15 transactions per second (TPS), Qtum's AAL enables 60 TPS (as of November 2018).

Qtum: Blockchain for Business Applications

On the official website of Qtum the authors advertise that Qtum is part of it.

> revolutionize the way smart contracts are viewed, developed and used. With the x86VM, QTUM will be the first blockchain platform to make next generation dApps a reality

operations (e.g. Bitcoin transactions), Ethereum allows them to create their own operations of any desired complexity. The core for this is the Ethereum ("EVM") or Qtum Virtual Machine, which can execute code of any algorithmic complexity. Developers can create applications that run on the virtual machine.

The Qtum x86 virtual machine is considered one of the greatest achievements of the project, as it is designed to remove barriers for developers and support popular languages such as C, C++, and Python. In addition, Qtum will provide a standard library for programmers that includes a set of pre-built operations and tools to simplify development. Ethereum lacks such a standard library, which means that developers must program their own solutions to recurring problems, which in turn slows development and potentially degrades security.

The use of the Qtum blockchain is freely available to everyone. However, the main focus of the Qtum Foundation is on Smart Contracts business applications. The aim is to facilitate the transition from legacy systems in ageing companies to blockchain-based solutions.

Qtum Oracles

In order to enable the use by the "real world" – the industry – Qtum, as well as Aeternity, supports "Oracles". External data can be provided to the blockchain via external devices and interfaces (APIs) so that this information can be used by the Smart Contracts on the Qtum platform.

Proof of Stake and decentralized Governance Protocol

Qtum uses a distributed governance protocol that enables variable blockchain parameters for smart contracts that can be changed **without hard forks**. This means that smart contracts can be developed with variable parameters such as block size (currently 2 MB), block time (currently around 120 seconds), gas price and gas limit.

Proof-of-Stake allows token owners to vote on network changes and upgrades. With this decentralized governance mechanism, Qtum wants to prevent hard forks. For example, if Qtum owners vote to increase the block size to 4 MB, the change will be implemented automatically. As is usual with proof-of-stake, node operators are rewarded for validating transactions.

Is it worth investing in Qtum?

The market for decentralized blockchain application platforms with smart contract functions is a highly competitive market. With the Enterprise Ethereum Alliance, which includes enterprise giants such as Microsoft, Intel, ING, Santander and many other global companies, Ethereum is currently in the best position to become the leading distributed application platform of the future.

The competition behind Ethereum is great. Above all EOS, Cardano, as well as Tron and NEO in Asia are already strongly developed platforms, against which Qtum has to compete. Nevertheless, Qtum is one of the most interesting cryptocurrencies on the market, with a working product that is already being used to develop distributed applications and ICOs. Qtum's future success will therefore depend to a large extent on how it can assert itself in industry (for business applications) and against its competitors.