Wanchain

Cross-chain smart contract and financial platform

Analyst: Louis Mareschi (@louismareschi)

Updated: May 18, 2018

Wanchain aims to create a new financial services industry centered around digital assets using cross-chain interoperability, privacy, and smart contract functionality.

Wanchain believes having an infrastructure that can connect these individual blockchains will unlock tremendous value and promote financial inclusion. In addition to facilitating cross chain transactions, Wanchain is an independent blockchain development platform. This allows for smart contracts, issuing tokens on the Wanchain network, and privacy protection mechanisms.

Project Overview

Name	Wanchain
Issuer	Wanchain Fdn. Ltd.
Category	Platform
Sector	Interoperability
Sale Start	10/03/2017
Sale End	10/04/2017

Token Overview

Name	Wancoin
Symbol	WAN
Type	Native
Initial Distribution	107,100,000
Current Supply	107,100,000
Max Supply	210,000,000
Emission Type	Fixed

Resource Links

- Website
- Twitter
- Reddit
- GitHub
- Telegram
- Whitepaper

Project Background

Wanchain is an open source project that is attempting to build a distributed blockchain based financial market. The team plans to achieve this goal through three pillars; cross chain interoperability, privacy, and smart contracts that give anyone the ability to create or access a suite of applications. Wanchain imagines use cases such as decentralized exchanges, lending, stablecoins, multi-currency payment and settlement, crowdfunding, and many other financial services will be facilitated on the network. The project was created in 2016 by Jack Lu, former co-founder, and CTO at Factom. Wanchain is currently being developed by the Wanchain Foundation, a non-profit organization registered in Singapore.

The project focuses on the growth of digital assets, including tokenization of traditional assets like stocks and bonds, and how they will interact with existing blockchains like Bitcoin and Ethereum. Wanchain plans to build a common framework, including cross-network interoperability, which will allow these different assets and their native ledgers to interact with each other. Initially, the team will focus on integration with Ethereum and plans to include interoperability with any public or private blockchain network.

Users can choose private transactions through the use of one time addresses, and the team plans to integrate ring-signatures, like those in Monero, in future releases. This is designed to provide the ability to transact privately and provide increased fungibility of assets.

Wanchain also runs an accelerator program called WANLab which seeks to support projects that are building on the Wanchain platform. To date, six projects have been picked for this accelerator program and will receive mentorship and resources from WANLab. Wanchain is part of the "Blockchain Interoperability Alliance," alongside the AION and ICON projects. The goal of this alliance is to promote interconnectivity between different isolated blockchain networks.

Technology

Wanchain is a fork of Ethereum and integrates similar smart contract capabilities. The platform uses proof-of-stake (PoS) for consensus but divides verification nodes into three groups; vouchers, storemen, and validators.

Nodes are required to stake Wancoin (WAN) in return for the ability to validate transactions on the network. They are compensated in the form of fees for this service. Any dishonest behavior causes their stake to be slashed. The platform aims to facilitate cross-chain interoperability using a series of locked accounts. When sending a cross-chain transaction, assets (value) are not flowing across chains. Instead, they are sent to a locked account that keeps funds on the original chain, akin to a deposit. Vouchers provide proof of transactions between the original account and the locked account.

Funds are then replicated on Wanchain, and a receipt is generated, showing how much a user can transact with. Locked accounts are created through a cryptographic method called secure multi-party computation (sMPC), which allows for coordination using a public-private address scheme. Storemen are responsible for operations related to locked accounts such as account generation and key management. Private keys are not exposed to a single individual during this process, but instead, are divided amongst multiple validators requiring some, or all, to reconstruct the data. This aims to also maintain network integrity if some of the validators are corrupt or offline.

Validators are general verification nodes that record transactions whenever there is consensus. By dividing the nodes into three distinct groups, the team hopes to reduce the chance of collusion.

Wanchain uses one time accounts and plans to use ring signatures to protect anonymity and fungibility in the network. Privacy can be provided for simple transactions (sending tokens from one wallet to another) and more complex operations with smart contracts and cross-chain requirements.

In Wanchain, every account has a main account that contains sub-accounts or one-time accounts. When a sender initiates a private transaction, they create a unique account for the recipient based on their public key. The sender sends the money to this one-time account instead of the public address. The recipient can then use their private key to access all their one-time accounts.

Ring signatures are a type of digital signature in which a group of possible signers are merged to produce a group signature. The sent transaction is mixed with a series of past transactions that act as a decoy, to prevent anyone from identifying the actual sender.

Ring signatures obfuscate the sender while one time accounts obfuscate the receiver.

Distribution

Wanchain completed a token sale in Oct. 2017. A pre-sale was held for strategic investors and raised approximately $13.0 million at a price of $0.32 per WAN. The following public sale raised $35.3 million at a price of $0.34 per WAN. The public sale cap of $35.3 million was reached in approximately 6 minutes.

A total of 210.0 million WAN was created as an ERC20 token, which was redeemable for a native token on Jan. 29, 2018. Investors, in both the pre-sale and public sale received 51% of total supply (107.1 million WAN). The team received 20% of supply (42.0 million WAN) and the Wanchain Foundation received 19% of supply (39.9 million WAN). A remaining 10% of supply (21.0 million WAN) was reserved for future network rewards.

Of the total amount raised the team indicated 60% would be spent on research and development, 10% on community development, 10% on marketing, 10% on infrastructure, and the remaining 10% on daily operations.

Roadmap

Wanchain had the first significant release of its platform, Wanchain 1.0, on Jan. 18th, 2018. This release supported privacy protection with one time accounts and also the first iterations of the Wanchain wallet and block explorer. The next major release, Wanchain 2.0 is planned for summer 2018. The main feature of this release will be cross-chain integration with Ethereum and a multi-coin wallet. The Wanchain team has been working very closely with Ledger, and full hardware wallet integration is expected around the same time.

Longer term, Wanchain plans to integrate cross-chain capabilities with Bitcoin by the end of 2018 and integration with private chains towards the end of 2019. Any blockchain that uses a public-private scheme will be able to connect with Wanchain in a permissionless environment without alerting the original chain.

Team

Jack Lu
Founder

- Co-founded Factom in 2012 and founded Wanglu Tech in 2016

Dustin Byington
President

- Co-founded Tendermint and founded Stokens Venture Capital

Advisors

David A. Johnston
Chairman of the Board at Factom

Feng Han
Secretary General of DACA

Albert Ching
Founder of i-Sprint

Ramble Lan
Chairman of North America Blockchain Association

Investors

Blockgrade Capital

Kingsley Advani

Limitless Crypto Investments

Additional Resources

- Blockgrade: Wanchain Analysis
- YouTube: State of Wanchain