

Zilliqa is a smart contract processing platform focused on transaction speed and scalability.

The project leverages sharding technology, which divides the blockchain into multiple processing layers, and a proprietary programming language to increase throughput. While Zilliqa hopes to offer fast smart contract processing, the tradeoff is a lack of contract features compared to networks like Ethereum.

Project Overview

Name	Zilliqa
Issuer	Zilliqa Research
Category	Platform
Sector	General purpose
Sale Start	12/27/2017
Sale End	01/10/2018

Token Overview

Name	Zilling
Symbol	ZIL
Type	ERC20 token
Initial Distribution	6,300,000,000
Current Supply	6,600,000,000
Max Supply	21,000,000,000
Emission Type	Fixed

Resource Links

- [Website](#)
- [GitHub](#)
- [Twitter](#)
- [Telegram](#)
- [Medium](#)
- [Reddit](#)
- [Whitepaper](#)

Project Background

Zilliqa competes with current smart contract processing platforms, such as Ethereum, NEO, and Stellar. The project takes a blend of approaches when targeting this niche, with some borrowed and some new concepts. The team's primary motivation in building this product was to create a platform that could process smart contracts at scale without sacrificing core blockchain principles. Unlike many highly scalable smart contract processing platforms, like NEO or EOS, Zilliqa does not rely on delegated proof-of-stake (DPoS) for its transaction throughput. While DPoS potentially allows for massive scaling it also centralizes the network in a way that many deem to be unsafe.

The key value proposition of Zilliqa is to create a network that is scalable and functional, while true to blockchain security principles. In order to achieve this the platform relies on sharding technology.

Zilliqa has yet to release its main network, but has released a public test network for developers. Once it has been rolled out the team plans to work with users to understand the best applications for high throughput blockchain technology. Underlying the platform is a programming language built specifically to handle applications that require high levels of complex computation. In particular, MapReduce functions, data science applications, and financial modelling are mentioned as use cases by the team, though they stress that their platform is versatile and can be used for many applications.

¹ Source: <https://paymentweek.com/2018-4-3-zilliqa-releases-first-sharding-blockchain/>

Technology

Zilliqa focuses on scalability through a process called sharding. While many current blockchain applications utilize every node on a network to process every transaction, Zilliqa divides the network into 10 shards, each processing one tenth of the network's transactions and requiring only one tenth of the miners at any given time. This reduces wasted computational resources related to nodes confirming transactions that may have already been verified by thousands of others.

Sharding is also applied to smart contract processing, in that only subsets of the entire network resources are used to perform any given computation. Using this technology Zilliqa expects their throughput to roughly double with the addition of every couple hundred miners.

Zilliqa uses standard proof-of-work (PoW) for security in its network, but it has a two-layer blockchain structure to allow for more efficient use of computing resources. To create an identity or participate in sharding on a user must show proof-of-work but this is not used to achieve consensus. Instead, Zilliqa employs a consensus protocol known as practical Byzantine fault tolerance. In this protocol, nodes are grouped with a leader that is responsible for broadcasting both transactions and decisions. When two-thirds of a leader's backup nodes cast their votes, the leader commits an answer. Leader nodes are changed continuously to prevent malicious leaders from having an undue effect on the network.

Unlike Ethereum, Zilliqa does not have a Turing-complete smart contract language. This means that there are only specific functions that the language can perform, making it less versatile. Other projects like Stellar have taken a similar approach as it can allow the language to be less redundant and capable of sharding. Zilliqa cites neural nets as being a prime example of a computation that would be best served by their language, as on any other network it would likely be prohibitively expensive.

In the future, Zilliqa plans to implement a significant number of new technologies including:

State sharding – Allowing the data stored by the network to be divided in the same way as the processing and consensus layers.

Secure Proof-of-Stake – A security mechanism that distributes consensus power to the most heavily invested nodes in the network.

Storage pruning – A mechanism for reducing the total amount of data required to store in order to participate in the network. This can eliminate spam and dated blocks from the required data.

Privacy preserving computation – Computation that removes the identity requirement of participating in the network, so computation is not tied to an account on the blockchain.

Distribution

Zilliqa completed a public token sale on the Ethereum network between Dec. 2017 and Jan. 2018. Participants in the sale received ERC20 Zilling (ZIL) tokens which will be converted to native tokens when the main network launches. The sale had a hard cap of \$22.0 million at a price of 116,060 ZIL per ETH. Initially, the project planned to raise up to \$20.0 million but adjusted the cap due to the rise in ETH prices.

Only members of the community Slack or Telegram channels before Nov. 29, 2017, were eligible to participate in the sale. Each community member was capped at a total of 2.5 – 5.0 ETH during the sale. Early supporters that provided funding or other support to the project were eligible for an extra 10 – 15% "bonus" allocation on top of the tokens they received through the sale.

A total of 21.00 billion ZIL were created, with 6.30 billion distributed through the public sale. An additional 6.30 billion tokens were allocated between Anquan Capital (2.10 billion), Zilliqa Research (2.52 billion), the founding team (1.05 billion), and various supporting agencies (0.63 billion), including Bitcoin Suisse. The remaining 8.40 billion tokens were reserved for future mining rewards, which will be distributed over a ten year period.

Tokens allocated to Anquan Capital, Zilliqa Research, the founding team, and supporting agencies, excluding Bitcoin Suisse, are subject to a vesting plan which releases new tokens quarterly over a three year period.

Of the funds raised in the token sale, \$17.6 million will go to research, development, and operations. Anquan Capital was allocated \$3.3 million of the proceeds, and the remaining \$1.1 million was rewarded to the founding team.

Team

Xinshu Dong

CEO

- Published scientist and practitioner in building secure systems
- Led the research and development of Anquan's proprietary scalable and secure blockchain, deployed for financial and ecommerce applications

Prateek Saxena

Chief Scientific Advisor

- Research professor in computer science at National University of Singapore
- PhD in computer science from UC Berkeley
- Received several premier awards such as the Top 10 Innovators under 35 (MIT TR35 Asia) in 2017

Saiba Kataruka

Marketing Lead

- Consultant with IBM for five years

Addison Huegel

Head of Communications

- Previously communications consultant to the Ethereum Foundation and DEVCON1

Yaoqi Jia

Head of Technology

- Experience building secure and privacy-preserving web and distributed systems with cryptographic mechanisms
- Research work has been published in top international conferences, such as CCS, USENIX Security, PETS, RAID, and ESORICS
- Received the Best Paper Award in W2SP (2014) and ICECCS (2014)

Amrit Kumar

Head of Research

- Research fellow at the National University of Singapore
- PhD from Université Grenoble-Alpes, France
- Engineer's diploma from Ecole Polytechnique, France, where he studied computer science and mathematics

Ong En Hui

Head of Business Development

- Previously held sales and distribution roles at BlackRock and JPMorgan Asset Management

Max Kantelia

Chief Evangelist

- Co-founder of Anquan Capital in Singapore
- On the board of Aeriandi and Untapt
- Selected by EY as one of Asia's Top 100 fintech contributors in 2016

Analyst: Robert Clark(@cryptodiplo)

Updated: April 16, 2018

4 of 4

Advisors

Evan Cheng

Engineering director at Facebook

Aquinas Hobor

Assistant Professor at Yale-NUS College and School of Computing

Alexander Lipton

CEO and founder of StrongHold Labs

Loi Luu

Developed Oyente and co-founded SmartPool

Nicolai Oster

Head of ICO at Bitcoin Suisse

Stuart Prior

More than 20 years in corporate and investment banking

Christel Quek

Co-founder of BOLT and founder of Pin8cle

Ilya Sergey

Researcher

Vincent Zhou

Founding partner at FBG Capital

Investors

1kx

8Decimal

DHVC

FBG Capital

Global Brain

HyberChain Capital

Kenetic Capital

One Block Capital

PolyChain

Signum Capital

Talenta

Additional Resources

- [Zilliqa Position Paper](#)
- [Blog: Details on Zilliqa's Token Generation Event](#)

This report has been prepared by a member of the Messari community and is for educational purposes only. Community members produce research on a voluntary basis and are not compensated by Messari. Messari is an open-source platform and these reports, along with the accompanying data, will be made available through messari.io and the soon to be launched Messari data library.

Reports published by Messari should never be considered investment advice, including but not limited to, an endorsement of a cryptoasset or a recommendation to buy or sell. The analyst that wrote this report maintains a position in cryptoassets, including the one covered in this report. Messari requires that employees disclose any holdings when reviewing or publishing community reports. This report was reviewed by Eric Turner, CFA. At the time of publication Eric had positions in bitcoin (BTC), ether (ETH), and dogecoin (DOGE).

Messari makes no guarantees to the completeness or accuracy of this information. If there is incorrect information in this report, please contact eric@messari.io, and we will update accordingly.