Research Report
July 2021

zilliqa

HILLRISE
RESEARCH

Introduction

In this report we present our coverage of Zilliqa, a high-throughput public blockchain platform and pioneer of sharding technology with deep connections to academia. Born out of the National University of Singapore in 2017 and a longstanding fixture in the upper echelon of crypto-asset valuations.

As a blockchain infrastructure project, Zilliqa's technology is designed to appeal to the scalability issues faced by other public blockchains. Their technology has been built to scale to a throughput of thousands of transactions per second (TPS).

Zilliqa's blockchain is said to be linearly scalable, meaning that the network is able to process more transactions per second as more mining nodes join the network. This notion of linear scalability is Zilliqa's primary unique value proposition in contrast to other well-known layer-1 designs. The technology and sharding backbone of Zilliqa is relatively sophisticated and as such and for the purposes of this report, we have not delved unnecessarily deeply into the intricacies of the sharding technology and the associated complexities. We aim to provide a level of detail sufficient to understand the concepts and impact of the tech.

MAINNET LAUNCH
2019

Zilliqa's mainnet was launched in early 2019 and is powered by the ZIL token. As of writing, ZIL is ranked as the 73rd largest cryptocurrency by market capitalization accounting for US $1.3bn of value.

As a mature blockchain project, Zilliqa has a rich ecosystem of products and initiatives. We have chosen to cover a distinct selection of major ecosystem items in favor of keeping this report concise.

History of Zilliqa

TRANSACTIONS TO DATE
>20m

Zilliqa was first conceived in 2017 by a group of researchers from the National University of Singapore with the goal of using "sharding" to achieve scalability, security, and decentralization in a public blockchain. Being Singapore-based, the project benefits from the country's robust and growing blockchain ecosystem. Their blockchain mainnet was launched in January 2019 and crossed 20 million on-chain transactions in June 2021. The ERC-20 token swap to the native ZRC-2 standard concluded on 15 February 2020. With an ICO price of $0.0035/ZIL, the token price traded at a low of $0.0024 on 13 March 2020 and peaked at $0.25 on 6 May 2021.

Introduction to the Blockchain Trilemma

The three recurring foundations of blockchain technology at its most fundamental level are (1) scalability, (2) security, and (3) decentralization. However, the 'Blockchain Trilemma' also suggests that you cannot achieve all 3 simultaneously – one must be sacrificed in favor of the others.

The Blockchain Trilemma

Scalability

Security

Decentralization

For instance, the Bitcoin network is known to be highly secure and decentralized at the cost of scalability, with a capacity for approximately 7 transactions per second. Ethereum 1.0 shares a similar issue while less severe at approximately 15 TPS. Alternatively, other networks like Ripple or Tron may be scalable and secure but are undoubtedly less decentralized.

MAX THROUGHPUT
2,828 **TPS**

In 2018, with 6 "shards" (3,600 nodes), Zilliqa's testnet was able to achieve a max throughput of 2,828 TPS. Visa is reported to handle approximately 1,700 TPS on average, but with a theoretically higher throughput (reportedly over 24,000 TPS)[1].

With security and decentralization the priority of many high-profile blockchain projects, several solutions have sprung up that claim to natively solve this trilemma or address it off-chain via a Layer-2 protocol. Whether on-chain or off-chain is the better solution is up for debate.

Zilliqa aims to achieve all three cornerstones through the use of network sharding to address scalability. Starting with a cap of 3 shards, which may be increased over time through protocol parameter adjustments.

However, it must be noted that there still is a lower level of decentralization relative to the Bitcoin and Ethereum networks due to the use of 'seed nodes'.

---

1   Visa. Visa acceptance for retailers. 2021. https://usa.visa.com/run-your-business/small-business-tools/retail.html.

Sharding

Here we introduce the concept of network sharding as a means to achieve scalability in blockchain architecture. Zilliqa's sharding process consists of (1) network sharding, (2) transaction sharding, and (3) computational sharding.

Network sharding involves dividing up all the nodes in the network into smaller groups called "Shards", where each shard can then process transactions "in parallel".

For example, 10,000 nodes split into 1,000 nodes per shard will have 10 shards each processing different transactions. The latter process is called **transaction sharding**.

MINIMUM NUMBER OF NODES PER SHARD

600

By virtue of this design, a growing network allows for linear scaling. This is in stark contrast to most networks that lose throughput as they expand. It is important to note that each shard must still contain a sufficient number of nodes (dynamically estimated with a lower bound of 600) verifying transactions to maintain security in the network.

Proof-of-Work (PoW) is introduced here to perform network sharding and provide resistance from Sybil attacks.

In a nutshell, Sybil attacks – commonly known as 51% attacks – occur when a nefarious entity tries to attack the network by gaining control of and manipulating consensus. Zilliqa's PoW solves this by making all new nodes perform PoW and have existing nodes authorize their entry, such that it is difficult for a malicious entity to run multiple nodes for nefarious purposes. However, as described in the next section, it is not used for consensus and validation.

Computation sharding allows applications to be run efficiently over the network by distributing the same or different 'subtasks' across varying groups of shards. For instance, some groups may perform sorting while others aggregate, all checking to see if they return the same outputs within their groups. This essentially provides the high-throughput required of computationally intensive applications to be executed on-chain while still maintaining consensus.

With Phase 0 of ETH2 implemented, conversations comparing both Zilliqa and Ethereum's sharding strategies can be expected to increase. At the moment, ETH2 validators are only finalizing empty Beacon Chain slots (Phase 0). But the Beacon Chain will form the heart of the ETH 2.0 system and will be responsible for coordinating the validation of the ETH shards once Phase 1 commences in the future, merging the current ETH network with the Beacon Chain. This will bring along sharding capabilities, expected to split the network up into 64 shards that will split processing transactions and computation. Alternatively, Zilliqa has no upper bound cap on the number of shards due to the way the network scales.

Both networks are similar in the way that they assign validators into each shard: Zilliqa's combination of 'DS Committee' and main chain vs Ethereum's Beacon Chain.

However, this is where NEAR Protocol, a new sharded smart-contract-based Layer-1 protocol differs from the pair by introducing shard "chunks" instead of "shard chains". No participant has to download the network's full state, instead only maintaining the state of the shard they participate in.

Consensus PBFT

Byzantine Fault Tolerance (BFT) stems from the Byzantine Generals' Problem first conceived in 1982, that talked about the difficulty in reaching a consensus decision given communication issues and potential malicious actors. BFT in a consensus system and in the context of a blockchain network allows the system to resist any failures such as malicious actors, and continue to operate well.

Zilliqa achieves consensus via a combination of PoW and practical Byzantine Fault Tolerance (pBFT). However, PoW is not used here in the conventional sense and is only used to establish node identities. pBFT also allows consensus to be achieved even with malicious actors in the network.

How does it work?

PoW is first used by each node to establish their identities. While it does not produce any block rewards like in Bitcoin, it helps to create Sybil-resistance. At the start of each DS Epoch (comparable to block time in Bitcoin or Ethereum), nodes compete to enter the Directory Service (DS) Committee through a fastest-first PoW process, then replacing the oldest node in the DS Committee (first-in-first-out basis).

Collectively, the DS Committee has been elected, the sharding process begins with the remaining nodes performing another PoW, which is then validated by the new DS Committee. DS Nodes are rewarded in ZIL tokens for their work.

Nodes are then assigned to their respective shards – a consensus group – where they will undergo a three-stage process. Within each shard, nodes are sequentially ordered with 1 leading or primary node ("leader") and the rest being 'backup' nodes.

Stage 1
Pre-prepare

Stage 2
Prepare

Stage 3
Commit

The leader begins by broadcasting the state of the blockchain (and "microblock") to all other nodes in its shard through a "pre-prepare" message.

Every node individually validates the microblock, then relays a "prepare" message to all other nodes.

Each node will receive the respective "prepare" messages, following which it will relay a "commit" message back to all other nodes. When all of the "commit" messages have been received back from its peers, the microblock will have been confirmed and is added to the final block.

Why pBFT?

KEY PBFT BENEFITS
Finality, efficiency, lower reward payout variance

pBFT brings about three key benefits: (1) finality, (2) efficiency, and (3) lower reward payout variance. With finality, each block proposed is final with an exact agreement, such that no confirmations are needed and the risk of temporary forks is removed (present in Bitcoin and Ethereum). The non-computationally intensive nature of Zilliqa's modified-PoW with pBFT makes achieving consensus much more energy-efficient as compared to traditional PoW systems.

PoW required for node identification is dynamically achieved and does not need to be run on a per-block basis. Finally, the collective decision-making process of pBFT allows the incentive layer to reward every participating node in contrast with traditional PoW that only rewards the leader.

As with anything, there are drawbacks. Zillliqa does not do 'state sharding'. State sharding is essentially allowing full nodes (that typically have a history of the entire network) to not store the entire network's history – reducing their storage and communication burden. This effectively increases throughput and theoretically the opportunity for the degree of decentralization (lower costs meaning that more participants can run a full node). With the team continuing to research state sharding, its implementation in the future may be possible, but will indeed prove difficult.

Scilla Programming Language

scilla-lang.org

Scilla, short for **S**mart **C**ontract **I**ntermediate-**L**evel **LA**nguage is the native programming language for the Zilliqa blockchain and ecosystem. Whereas many programming languages such as Solidity for Ethereum require a relatively deep understanding and extensive auditing, Scilla is built specifically with smart contract safety and usability front of mind.

Safe-by-design

As you may have noticed over the past few years, some blockchains – including Ethereum – have seen some very large hacks, exploits, or simply mistakes from developers. These have often led to funds being transferred to malicious actors or being effectively lost in a locked contract.

It's not fair to attribute the aforementioned to the specific blockchain networks or technology, however, it's perhaps more relevant to look back a step prior, to the programming language allowing developers to introduce flawed logic to begin with. Scilla tackles this by differentiating between communication on one hand (blockchain transactions and messages) and on the other computation (logic and calculations).

In essence, this comes down to separating the 'contract' and 'blockchain' when it comes to logic.

ⓘ **Fun fact: Scilla was designed for Zilliqa, but can be used with any other blockchain.**

Zilliqa Ecosystem

Here we will highlight several key areas of development within the growing Zilliqa ecosystem. A community directory has been set up to collate the growing environment of projects and initiatives at zilliqaproject.com. This is a regularly updated list of projects which at the time of writing is over 40+ projects strong. In the following sections, we will be covering some of the notable names in the ecosystem.

Zilliqa Capital
zilliqacapital.com

A proposed US $50-200m investment hub that aims to accelerate growth and become the key investment platform within the Zilliqa blockchain ecosystem.

This capital will be strongly focused on the next generation of FinTech, open finance, and DeFi within the APAC, ASEAN, and Indian regions.

ZilHive
zilhive.org

ZilHive is an initiative by Zilliqa and several partnered companies, projects, and incubators. The goal of the initiative is to enable more people to work with Zilliqa, utilize Zilliqa's tech, and learn about the broader ecosystem. The program is based on three core pillars: education, grants, and an accelerator. ZilHive also has an additional incubator and venture capital arm.

Education
The ZilHive initiative hosts a series of educational content, including LearnScilla, a website (and course) that allows anyone to pick up on learning the native Zilliqa safe-by-design smart contract language. An understanding of Scilla enables front row eligibility when it comes to ZilHive grants. There is also an established community for Scilla learners and developers for added motivation and collaboration.

In mid-2019 Zilliqa offered students of King's College London a free, four-week blockchain 'A-Z' program in collaboration with a student association at the college. Allowing students to get a good grip on blockchain as well as an impression of what it's like to work with industry players.

Grants
The ZilHive grants program was established as a means of incentivization and encouragement for developers to build their dApps on top of the Zilliqa blockchain. Some notable companies that have received grants (and support) from the ZilHive grants program are Zengo, Unstoppable Domains, and Viewbase.

Since the inception of the program 9 'waves' of grants have been handed out, funding over 90 projects with developers from more than 22 different countries. As of writing, the total pool for the program is over US $5m and the 10th wave is in progress.

Accelerator and funding

The ZILHive accelerators help potential blockchain startups enter the Zilliqa ecosystem by providing them with individual support tailored to their specific needs and roadblocks. This can be anything from legal assistance to helping a startup with the execution of a proof of concept all the way up to helping them structure their fundraising process.

The projects partaking in the accelerator are supported by a wide range of industry veterans and established stakeholders, companies and projects, including **Binance**, **Torus Labs**, **Zengo**, **IOSG Ventures**, and many more.

Zillacracy
zillacracy.com

Currently, Zillacracy is a fully community-owned project aimed at aiding and supporting development on the Zilliqa blockchain to grow the network. Members are encouraged to contribute to various initiatives through both technical (e.g. adding to the Scilla codebase or developing a dApp) and non-technical means (e.g. creating marketing material such as infographic explainers).

Contributors may apply and receive grants from the Zillacracy Council to support their projects. As of writing, 10 projects have been completed, with 5 in progress and 9 remaining open. Some Zillacracy grant recipient projects are **Red Chillies**, **Qvote**, **Xcademy** and the **Learnblockchain** platform.

The Zillacracy Council is a group of 6 who are a mix of motivated community participants and core Zilliqa team members. In the near future, Zillacracy will move towards a Decentralized Autonomous Organization (DAO) model. Additional information on the new structure should be available soon on Zillacrazy socials.

Xcademy
xcademytoken.com

XCAD NETWORK

Xcademy is a crypto-focused, Youtube-based influencer academy that Zilliqa has made an investment in. Creators will be able to directly monetize their content through cryptocurrency and incentivize their audience using tokenization (think celebrity tokens).

This initiative will help narrow the gap between crypto-natives and mainstream audiences. With NFTs being all the buzz, a heavy focus on NFTs will be key to its success.

Xcademy has notably secured investment from MrBeast and KSI, as announced in May 2021.
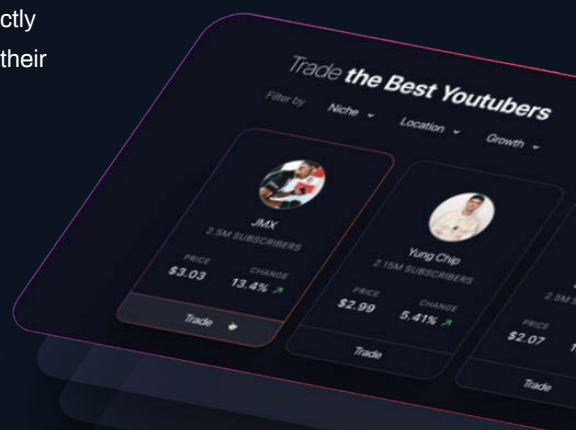
Built on Zilliqa

Here we will explore and unpack several notable products, protocols, and areas of development that incorporate key components of Zilliqa's technology.

ZilSwap
zilswap.io/swap

ZilSwap is Zilliqa's first DEX for the ZRC-2 token standard, which has been built by Switcheo, a Singapore-based cross-chain DEX that has raised funds from the likes of **DeFiance Capital** and **NGC Ventures**.

Modelled after Uniswap with a fittingly similar interface, ZilSwap represents the network's first push into the burgeoning DeFi space. Other features are similar such as the use of the constant product automated market making (AMM) architecture and 0.3% swap fees for all liquidity pool providers.

ZilSwap's first pool launched with the ZIL-XSGD pair and allows users to swap ZIL for the first Singapore-Dollar-backed stablecoin built by Xfers. As of writing ZilSwap has approximately 20 registered liquidity pools for different Zil-based tokens.

TVL ZILSWAP (03/2021)
$115m

As of 14 March 2021, ZilSwap's TVL surpassed 1inch's TVL at ~$115m, a significant feat considering its nascence. With the ETH/ZIL bridge coming up soon, there will likely be a wave of bridged assets flowing into the Zilliqa ecosystem as demonstrated by the sudden surge of assets into Binance Smart Chain and other Ethereum Layer-2s (L2).

ZilSwap's native ZWAP token was also launched via their Lightning Incentivisation program, similar to liquidity mining programs found across most DEXs such as Uniswap or SushiSwap. No doubt this has been a strong contributor to TVL growth in ZilSwap. The ZilSwap initial launch offering (ZILO) is planned for Q3 2021.

NFTs

Growing the NFT market on Zilliqa is another key focus. The ZRC-1 standard (ERC-721 equivalent) is ready to capture a primarily Ethereum-based NFT market through significantly lower minting and transaction fees.

Mintable.app is a leading NFT platform that allows users to mint and list NFTs on both Zilliqa and Ethereum. In March 2021, Mark Cuban invested an undisclosed sum into the Mintable platform.

Rapper Soulja Boy also partnered with Zilliqa to create the first audio-visual NFTs on the ZRC-1 standard. Several well-known football players (including Diego Costa and Pepe) partnered with Zilliqa to create a football NFT marketplace (**football.zilstars.com**) that as of writing has achieved over US $1.2 million in trading volume.

Unstoppable Domains

www.zilliqa.com/ecosystem/unstoppabledomains

Unstoppable Domains introduces unseizable and uncensorable web domains stored on blockchains. Initially integrated with Ethereum via the ERC-721 standard, it is now also integrated with Zilliqa after the Zilliqa Foundation launched its US $250,000 grant program in partnership with Unstoppable Domains.

The project is replacing long hexadecimal blockchain addresses with human-readable names, for example, **hillriseresearch.eth** or **hillriseresearch.zil**.

Ease of access for the non-crypto-native crowd and enabling free speech are central to the project's design considerations. Both regular and premium .zil domains can be bought for US $10 and $250 respectively.

Pillar Protocol
pillarprotocol.com

Pillar Protocol is a USD-pegged stablecoin protocol built on the Zilliqa network that uses gZIL for governance and reward allocation instead of a native Pillar governance token.

Typical of current stablecoin protocols, minting Pillars requires over-collateralization and will liquidate collateral should collateralization ratios exceed limits. Auction/Liquidation Oracles (ARO) will help maintain the stablecoin peg through exploiting the protocol's economic incentives.

In addition to deciding the types of assets that can be deposited into vaults, gZIL holders may benefit from price appreciation should liquidation occur. Currently, 70% of liquidation penalties (starting at 10% of liquidated capital) will be used to market-buy and burn gZIL.

The guarded mainnet test launch commenced on 6 April 2021.

RedChillies
github.com/RedChillies-Core/RedChillies-IP/blob/main/Whitepaper.md

RedChillies is a gaming (gambling) platform built on the Zilliqa network that has recently launched its mainnet. Their first game is an English Premier League betting service and will launch Ludo Dice, "Poker", "Racing", and "Shooter" in the future. Users can bet and win ZIL tokens, and will use the native "REDC" – a ZRC-2 token – for gas fees, voting, hosting games, and rewards.

Other projects

Zilliqa unveiled 8 new projects during the SWITCH 2020 event at the Singapore Blockchain Village with use cases such as asset tokenization, custody, and compliance. For more information, see the **Zilliqa** and **ZILHive** Twitter pages.
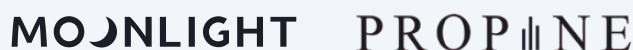
Notabene
notabene.id

Notabene is a risk management platform providing software, tools, and data that helps manage counterparty risk and allows customers to transact in cryptocurrency with confidence and ease.

Moonlet
moonlet.io

Moonlet is a non-custodial digital asset wallet enabling secure management and staking of crypto-assets that is mobile-app ready and Ledger compatible. Moonlet has over 7,000 users and 3,500 delegations.

Lumiere
www.lumiereproject.io

Lumiere is a film tokenization platform striving to boost liquidity, accessibility, and to mitigate risk in the film investment space.

Mugglepay
mugglepay.com

Mugglepay provides a software development kit (SDK) to merchants that accept cryptocurrency payments. Enabling far more cost-efficient cross-border transactions, while also allowing for stablecoin usage.

RupiahToken
rupiahtoken.com

Indonesia's most widely-adopted Indonesian rupiah-backed stablecoin, recently integrated with Mugglepay and Moonlet wallet.

CommX
www.commx.io

CommX is a democratized investment platform for art and real-estate through tokenization and fractionalization of digital assets.

Moonlight
www.moonlightwork.com

Moonlight is an employment platform that provides a zero-trust global working environment, enabled by their decentralized identity platform Vivid.

Propine
www.propine.com

Propine is a Monetary Authority of Singapore (MAS) regulated STO platform providing compliant end-to-end tokenization and custody solutions.

Partners

Hg Exchange
hg.exchange

Hg Exchange (HGX) is a private equities exchange formed by an alliance of financial intermediaries that are licensed and regulated by the MAS. HGX is live and accessible through member financial institutions, including PhilipCapital, PrimePartners, and Fundnel.

HGX is the first Zilliqa project to utilize its safe-by-design smart contracts, allowing the exchange to trade equities in a more efficient and transparent manner. Opening up the market to more companies and users, while lowering barriers to entry.

PRIVATE INVESTORS

500k

The platform allows private companies to issue shares, for example, employee share options and stock issuance. The platform is also well suited to handle share monetization and the creation of liquid markets. HGX sports over 500,000 private (and accredited) investors and a range of institutional users.

Xfers
www.xfers.com/sg

Xfers is a regulated provider of e-money and e-payment services in Singapore with a WASVF (Widely Accepted Stored Value Facility) approval by the MAS, offering flexible payment products and solutions for personal and business needs. The companies aim to drive equal opportunities and cost-saving solutions for digital businesses looking to set up in the region. Their investors include Y Combinator, 500 Startups, Eduardo Saverin, Tribe, and Golden Gate Ventures.

The Xfers solution is powered by Zilliqa, using Zilliqa's Scilla smart contracts to increase efficiency, transparency, and to make life harder for malicious actors. The smart contracts make sure that both parties fulfill their duties before making payouts and ensures (cross-border) settlement in minutes instead of days.

Xfers and Zilliqa have also teamed up to launch the 'StraitsX' or 'XSGD' stablecoin, which is pegged to and backed by the Singapore Dollar (SGD) on a 1:1 basis. The stablecoin initiative has achieved significant milestones recently including $100m in on-chain transaction value on the back of over SGD $10m XSGD issued. The XSGD will be a key enabler for South East Asian participation in the cryptocurrency markets.

Aqilliz

www.aqilliz.com

Aqilliz is a technology company that exclusively utilizes the Zilliqa blockchain as the infrastructure provider for its clients, meaning that any blockchain services the company offers will utilize the Zilliqa blockchain. This in turn provides any product with greater trust, transparency, and convenience.

The company currently provides a suite of marketing solutions that enable companies to restore the balance between brands, platforms, and consumers. This is achieved by creating a collaborative marketing ecosystem based on principles such as compliant data-sharing, targeted audience discovery, and optimized audience engagement.

Poly Network

www.poly.network

Poly Network is independently building blockchain interoperability between chains such as Zilliqa, Ontology, Ethereum, Elrond, and more. The project is enabling more generic cross-chain transfers and communications than just asset transfers. For instance, they envision the ability to pay dividends on Zilliqa for the ownership of an asset on Ethereum.

Zilliqa will work with Poly Network to build cross-chain capabilities, benefitting ecosystem participants through lower fees and developers with easily integrated Scilla-based cross-chain smart contracts.

Rosetta

www.rosetta-api.org

Rosetta is an open-source standard created by Coinbase to make integrations with public blockchain infrastructure faster, easier, and more reliable. The core of Rosetta is a growing set of APIs coupled with SDKs that have been widely contributed to by more than 8 teams since launching in September 2020.

ZIL Token

Tokens in the Zilliqa platform are called "Zillings" or ZILs for short and are the native asset of the Zilliqa network. The token fuels the network and is fundamentally used as an incentive for miners and as a payment mechanism for gas fees – for smart contract execution.

Key metrics (as per 15 June 2021)

CIRCULATING SUPPLY
12,122,747,934

LOCKED IN STAKING 🔒
5,098,978,779

OUT OF CIRCULATION
8,877,252,066

MINTING PERIOD
10 years

TOTAL LOCKED
5,641,670,411

ZIL PRICE
$0,1118

CURRENT VALUATION
$1,356,268,567

LOCKED IN ZILSWAP
461,706,377

DILUTED VALUATION
$2,352,000,000

LOCKED IN PANCAKESWAP
80,985,255

CURRENT VALUATION IN DEFI
$620,583,745

YTD PERFORMANCE
▲**35%**

ERC-20 LAUNCH, SWAP TO NATIVE ZIL
February 2020

Types of Zilliqa Nodes

Lookup nodes

Full nodes that have a copy of the network's history, share data with new nodes and dispatch transactions to shards and the DS committee.

Shard nodes

Mining nodes within the network that process transactions and are determined every block by the DS committee through the PoW process.

Directory (DS) Nodes

DS Nodes are essentially shard nodes with the additional task of aggregating microblocks to form the main transaction block and creating the DS Block for each new DS Epoch. Collectively, DS Nodes form the DS Committee.

Seed Nodes

Similar to Lookup nodes, but rather they do not dispatch transactions, instead they are mainly used for serving JSON-RPC requests (e.g. creating new transactions). Seed Node operators are required to stake a minimum of 10m ZIL tokens either by themself or with ZIL delegated to it by other nodes.

Staked Seed Nodes (SSN)

Seed nodes run by staking partners that serve requests from the community and receive ZIL rewards based on their performance as SSNs.

ZIL Token Utility

As introduced prior, the use of the ZIL token is similar to other smart-contract-based networks like Ethereum: as payment (gas) for transacting on-chain or interacting with dApps, and as block rewards for miners/stakers.

Staking

The easiest way for users to begin securing the network and earning ZIL/gZIL rewards is by staking through the Zillion portal. Users can sign-in either as Delegators or Operators and can enter via (1) Keystore, (2) Ledger, or (3) ZilPay.

STAKING APY
13.8%

As of writing, the estimated real-time annual percentage return is 13.8% excluding gZIL.

Block Rewards

With the implementation of ZIP-11, (1) global block rewards increased by 40%, (2) the share of block rewards for SSNs increased from 5% to 40%, while (3) miners fell from 95% to 60% (net fall from 95% to ~84%).

Furthermore, gas fees no longer exclusively accrue to miners but are now paid out in a 60/40 manner to miners and seed node operators, respectively.

gZIL Governance

Zilliqa's governance token gZIL was launched on 14 October 2020 as a way of rewarding long-term ZIL holders and having their voices heard. At the moment, users can only stake their ZIL in a non-custodial fashion through the Zillion platform. Undoubtedly other staking portals will be developed in the future.

1 YEAR DISTRIBUTION

722,700
gZIL

Starting 14 October 2020, a fixed 722,700 gZIL will be distributed over the course of 1 year only. For every 1,000 ZIL distributed to stakers, 1 gZIL will also be distributed. However, the amount of gZIL actually earned by respective stakers will depend on how long they have staked for, how much is staked, and how often they engage and interact with the Zilliqa network.

The Zillion staking platform also provides stakers with the necessary information such as (1) estimated real-time APY, (2) the relative percentage of total ZIL staked, (3) personal amount staked, (4) gZIL minted and total, and (5) the number of delegators and Staked Seed Nodes.

On 15 January 2021, the Governance Portal was launched, allowing the community to begin actively partaking in governance.

Tech Strategy

As of June 2021, the Zilliqa team is working on several R&D projects focussed on improving the core infrastructure of Zilliqa 2.0. Focus areas of further development are (1) protocol robustness, (2) backend efficiency for persistent storage, (3) improvement of the decentralization of the storage layer of historical data, (4) improving processing efficiency of smart contract sharding, (5) developing an off-chain/layer-2 solution, (6) cross-chain solutions for interoperability, and (7) zk-SNARKS support for privacy.

The team is also working on making Scilla more developer-friendly and on improving its execution engine. In order to make development on Zilliqa more accessible the team is developing a resource hub together with the SDKs, a developer toolkit, and documentation development.

ZIL/ETH Bridge

Zilliqa is developing an interoperability bridge with Poly Network. The ZIL/ETH bridge is expected to be completed by the end of Q3 2021 and will bring interoperability between Zilliqa and other chains most notably Ethereum, Bitcoin, and Binance Smart Chain. Its completion is expected to bring greater adoption to the network, opening up more opportunities for dApp creation and cross-chain capabilities to exploit Zilliqa's strengths.

Decentralized Finance

Immediate Future (6-12 months)

Zilliqa hopes to build and implement: (1) USD stablecoin based on ERC20-BUSD via Ethereum - Zilliqa bridge, (2) basic lending protocol, (3) margin trading platform built on ZilSwap.

While not from the Zilliqa in-house development team itself, Pillar Protocol (discussed prior) aims to create a DAI-esque stablecoin and could easily pivot to create a lending protocol too.

Short-term (12-24 months)

The team intends to build on several of the immediate goals including: (1) multi-currency stablecoins, (2) mainstream payment integrations, (3) asset tokenization, (4) decentralized identity, (5) unsecured borrowing/lending via (4), and (6) analytics.

With the creation of Xfer's XSGD and potentially Pillar's USD stablecoin, achieving their first mid-term goal appears feasible. Asset tokenization may be achieved via Hg Exchange (previously mentioned).

TyronZIL is a new project aiming to achieve the fourth goal of establishing a decentralized identity solution through their proprietary decentralized identity (DID) system.

Long-term (24 months and beyond)

Goals for the longer term include several high-impact relevant products and services for the broader industry including: (1) multi-asset support for asset and wealth management, (2) insurance solutions, (3) derivatives markets/solutions, (4) an orderbook-based DEX, (5) gZIL DAO, and (6) decentralized oracle solution.
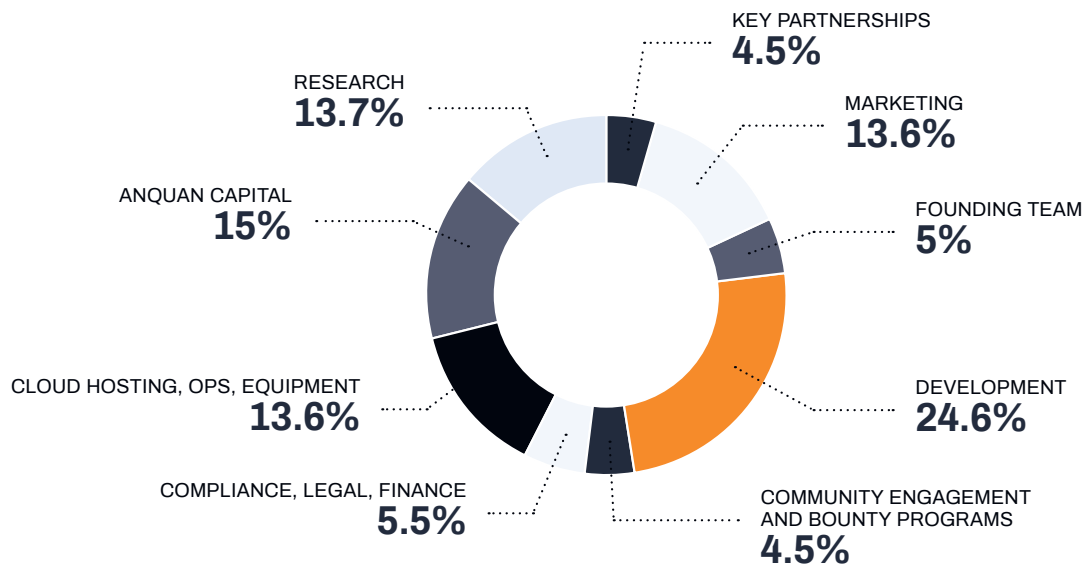
Token Distribution

Initial token distribution

An initial token supply of 6.3bn ZIL (30% of 21bn max supply) was minted at ICO, with 27.3% and 2.7% of the max supply sold in the private and public rounds respectively. At prices then, a total of US ~$20.5m was raised. 40% of tokens allocated to ZIL mining is expected to be distributed until 2040, varying based on the rate of decrease in "Guard Nodes" (nodes created in the project's early stage for safeguarding purposes).
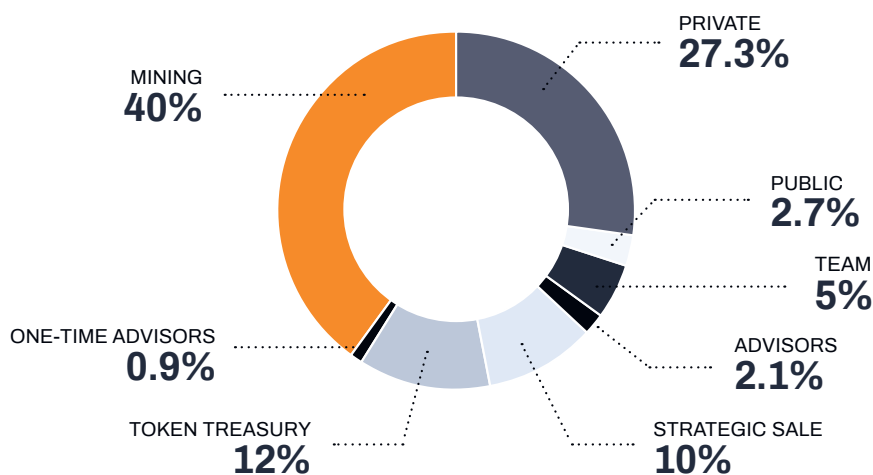
While there is currently ~14.7bn ZIL minted and circulating (as of writing), in reality, it is closer to ~12.5bn net of ZIL locked in multi-sig wallets and frozen in token swaps.

Allocation of Funds

The team has committed its funds raised across a wide variety of areas, including development, marketing, research, and cloud hosting. Notably, Anquan Capital (Zilliqa Research) was allocated 15% to fund new ventures in support of the Zilliqa network.

KEY PARTNERSHIPS
4.5%

RESEARCH
13.7%

MARKETING
13.6%

ANQUAN CAPITAL
15%

FOUNDING TEAM
5%

CLOUD HOSTING, OPS, EQUIPMENT
13.6%

DEVELOPMENT
24.6%

COMPLIANCE, LEGAL, FINANCE
5.5%

COMMUNITY ENGAGEMENT
AND BOUNTY PROGRAMS
4.5%

Zilliqa's Layer-1 Positioning

Technologically speaking Zilliqa is taking a strong position amongst current layer-1 protocols. Being built from the ground up with sharding in mind it forms a strong alternative to market leader Ethereum. Ethereums bid for scalability through sharding in Eth2, which further legitimizes Zilliqa's approach, and will remain a unique value proposition until Ethereum's sharding implementation.

In terms of ecosystem development Zilliqa has established robust structures amongst others in the areas of incubation (Zilliqa Capital, ZilHive), development support (Zillacracy), and liquidity (ZilSwap).

Zilliqa's unique smart contract language provides an easy and safe alternative to Ethereum's Solidity, and is applicable on other blockchains as well. Which could both work in Zilliqa's advantage due to Scilla's unique capabilities, and to their disadvantage with Solidity being the standard smart contract language for developers at the moment.

Team

Max Kantelia

CEO of Anquan Capital and Cofounder of Zilliqa and Aqilliz

Max has a background in computing and information technology. Max was CEO and co-founder of Anquan Capital. He was – and currently is also – the Director of the Board for Speik, a company specializing in voice applications before co-founding Zilliqa in 2017. Since co-founding Zilliqa, Max has also co-founded Aqilliz – a marketing tech company that builds on the Zilliqa blockchain.

Colin JG Miles

CCO

Colin has a background in various directorships and blockchain-related roles and has worked in a myriad of different positions at an executive level within marketing and sales. Starting with Zilliqa as Head of Marketing in February 2020 and since moving on to become CCO currently.

Amrit Kumar

President and CSO

Amrit has a background in mathematics, cryptology, and information systems. Amrit previously held several positions as a researcher, in particular at the University of Calgary and the National University of Singapore.

Prateek Saxena

Cofounder of Anquan Capital and Zilliqa

Prateek has a background in computer engineering and computer science. He has previously co-founded Anquan, a company building distributed ledger technology solutions and trusted computing platforms for financial markets. Prateek is also an Assistant Professor at the National University of Singapore.

Antonio Nocolas Nunez

Senior VP, Platform Engineering, Cofounder

Antonio has a BS in physics and computer engineering. Has previously held several software engineering positions, amongst which senior software engineer at Anquan Capital before moving to Zilliqa.

Investors

Kenetic Capital

Co-founded by Jehan Chu, Kenetic Capital is a venture capital firm based in Hong Kong. The firm has a strong track record of investing in stellar crypto-startups. The company often invests in both tokens and equity.

One Block Capital

Founded by Jack Huang, One Block Capital is a blockchain investment and advisory firm based in Hong Kong and has a focus on bridging the gap between cryptocurrencies and traditional financial markets.

IOSG

Founded by Jocy Lin, IOSG is a research and community-driven venture capital firm based in Hong Kong with a focus on layer-1 blockchains, middleware, and DeFi. They closely work with developers and DAOs to support entrepreneurs in the blockchain space.

Anquan Capital

Founded by Max Kantelia, Juzar Motiwalla, and Prateek Saxena, Anquan Capital is a collective of companies and projects including Zilliqa, Aqilliz and Anqlave. Anquan have deep expertise in fintech and blockchain and work with notable partners such as German TEN31 Bank.

NGC Ventures

Founded by Roger Lim, Tony Gu, Tony Tao, and Wayne Zhu, NGC Ventures or NEO Global Capital is a venture capital firm based in Singapore with a focus on adopting the best practices from the traditional investing space and bringing that expertise to crypto-assets.

Conclusion

Since their inception in 2017, Zilliqa has heavily broadened its scope and ecosystem. There is strong community participation within ecosystem development (e.g. Zillacracy). Having implemented sharding from the start this creates a unique positioning for Zilliqa amongst current layer-1 blockchain protocols. This advantage will not last forever as Eth2 is to be expected in the near future.

The number of projects and companies involved in addition to the ties with many reputable hackathons and more makes for a lively ecosystem. However, we still see that there are big leaps to be made in terms of adoption. By comparison, Zilliqa recently passed 20 million on-chain transactions since its inception, whilst Ethereum processes on average 1 to 1.5 million on-chain transactions per day.

Other layer-1 protocols have adjusted their positioning to welcome Solidity development and EVM integration, anticipating Ethereum's continued market leadership especially after its Eth2 launch. It might be challenging for Zilliqa to capture a sizable portion of the market without EVM compatibility to make sure that Zilliqa can also thrive in a cross-chain world that might just be spearheaded by Ethereum after all.

HILLRISE
RESEARCH

Hillrise Group is an independent venture capital and consulting firm comprising Hillrise Ventures and Hillrise Research, two distinct brands supporting emerging Web3 startups. Hillrise Ventures is a private investment arm providing ambitious Web3 startups with early-stage venture capital. Hillrise Research is a publisher of objective fundamental research bringing simplicity to complex technology.

https://hillrise.group

admin@hillrise.group