ALEPH ZERO

ECOSYSTEM

Value Proposition

ALEPH ZERO IS A PRIVACY-ENHANCING PUBLIC BLOCKCHAIN. BASED ON AN ORIGINAL PEER-REVIEWED CONSENSUS PROTOCOL AND AN INTEGRATION WITH THE SUBSTRATE STACK, IT SOLVES THE SHORTCOMINGS OF CURRENT DISTRIBUTED LEDGER TECHNOLOGY PLATFORMS: SPEED, VALIDATION TIME, SCALABILITY, AND SECURITY.

With wide-range of potential applications, Aleph Zero can operate as a public ledger as well as a private instance connected to the public ledger. This allows enterprises to build decentralized projects that benefit from the speed and security of a public DLT platform while still being able to preserve the privacy of their transactions.

> We see Aleph Zero's protocol as a masterpiece in privacy-preserving distributed ledger technology development

Vilma Matilla, founding partner of Node Kapital, a Strategic Advisor to European Union's Blockchain Observatory and Forum, and a Consulting Information Technology Specialist to the United Nations Association of the USA.

Core Features

> SCALABILITY

~ 100,000 TPS in a fully decentralized system*
* in a test environment, on 112 nodes spread across five continents

> PEER-REVIEWED

~ The Aleph Zero Consensus Protocol has been officially peer-reviewed and accepted for publication in the conference proceedings of Advances in Financial Technology 2019

> NEAR-FREE VALUE TRANSFER TRANSACTIONS

~ Simple value transfers are as close to being free as possible

> DECENTRALIZED

~ While Aleph Zero is DAG-based, it implements a large, rotating, and random committee to achieve proper decentralization

> COMMON WALLET & DECENTRALIZED EXCHANGE (DEX)

~ Using advanced cryptography, exchange you Bitcoin, Ethereum, and other digital assets on non-custodial peer-to-peer decentralized exchange

> PRIVATE SMART CONTRACTS

~ Customize functionality for automatio and programmable contracts

> HUB AND SPOKE MODEL

~ Sync your application to Aleph Zero's ledger

> FILE STORAGE

~ Application Programming Interface (API) hooks that allow seamless integration into InterPlanetary Fill System (IPFS) as well as proprietary data solutions.

Further details about the platform will be published in a Platform Whitepaper.

ALEPH ZERO

Executive Summary

BUSINESSES, DEVELOPERS AND TECHNOLOGICAL SOLUTIONS SHOULD GIVE CONSIDERATION TO ALEPH ZERO AND THE POTENTIAL OF DISTRIBUTED LEDGER TECHNOLOGY (DLT) TO MEET THEIR SCALABILITY AND DECENTRALIZATION NEEDS.

The Aleph Zero protocol is easy to interface with and transparent, allowing businesses' solutions to be more efficient, powerful, and trustless. Our protocol is backed by a novel scientific paper that presents years of research from experts in the fields of cryptography, mathematics, and other disciplines, culminating in the creation of a thorough solution to the problem of how to transmit data and value across networks with high throughput and quick confirmation in a decentralized manner. The scientific paper allows Aleph Zero to be fully verified as valid by trained experts in the domain of mathematics and cryptography.

We invite everyone to review our research and participate in the discussion.

Now is the time for a "post-blockchain" protocol that adheres to the progressive principles set forth by Satoshi Nakamoto. Since the launch of blockchain in 2009, a decade ago, research has moved forward and improved ways of achieving the promise of a vibrant decentralized world. We're concerned that the state of DLTs is slowly moving towards centralized, permissioned, and leader-based environments in which a small number of individuals are in control of each network, thereby creating liabilities and single points of failure. In contrast, at Aleph Zero, we cultivate an open culture, a scientific approach, and a constant flow of ideas that can guarantee true progression of the domain.

The core of Aleph Zero is a new algorithm built using the technology of a Directed Acyclic Graph (DAG) to create an efficient and decentralized system. It exceeds industry competition by using a practical approach to the transfer of value and the extensibility of smart contracts. Regardless of the number of other transactions, the validation times are always fast. Aleph Zero is what decentralized technology should look like at the protocol level, and will usher in a brighter future for businesses and technology seeking large amounts of data exchange and fast confirmations.

It also allows for customizable business solutions which interact with other parties and allow for settlement on a truly decentralized ledger proving the authenticity of centralized records. We use the "hub and spoke" model, which allows businesses to have a spoke, or private instance, that interacts with the main decentralized ledger. With this, businesses can interact with each other in a trustless manner efficiently and cheaply while still maintaining their own private network.

In it's Golang implementation, Aleph Zero achieved validation times of 416 miliseconds for a simulated amount of 89'600 transactions per second (TPS) in an environment consisting of 112 Amazon Web Services (AWS) nodes spread across five continents.

The current implementation is built in Rust to allow for an integration with Parity's Substrate technology stack. Technically, the language is more performant, however, the integration itself might lower the numbers achieved in the test results.

Overall, the goal of Aleph Zero is to make it possible for SMBs and enterprise to communicate at a rate close to what they would expect with regular internet communication while still utilizing the benefits of decentralization.

Ecosystem

Aleph Zero is an ecosystem that consists of:

- **AlephBFT Consensus**
  - ~ A novel DAG protocol
- **Aleph Zero Cloud**
  - ~ Decentralized file storage / IPFS
- **Private Smart Contracts**
  - ~ Scalable, self-executing, private smart contracts
- **Common**
  - ~ Decentralized Exchange (DEX) with a trustless universal wallet
- **Liminal**
  - ~ Multichain privacy layer usable across all networks that bridge to Aleph Zero
- **Future infrastructure use cases**

PROJECT: ALEPH ZERO

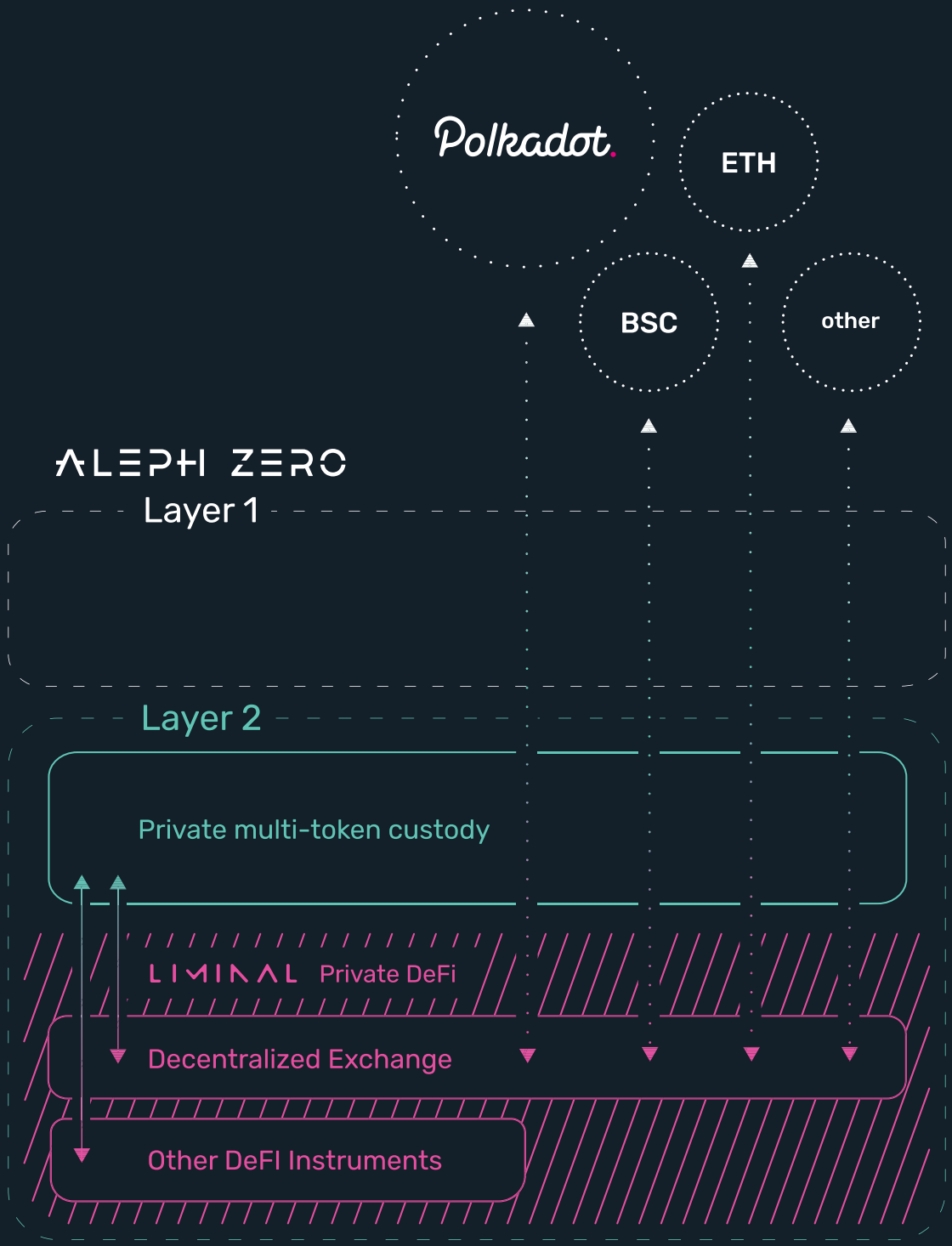
FOUNDATION: ALEPH ZERO FOUNDATION

PRODUCTS: common. LIMINAL

PROTOCOL: ALEPH BFT

COIN: $AZERO

The first product that is being built on top of the platform is Liminal – a multichain privacy solution.


Polkadot.
ETH
BSC
other
ALEPH ZERO
Layer 1
Layer 2
Private multi-token custody
LIMINAL Private DeFi
Decentralized Exchange
Other DeFI Instruments

Why we are Building ALEPH ZERO

THE ALEPH ZERO TEAM IS AN ASSEMBLAGE OF HIGH ACHIEVERS. WE SEEK TO CREATE NEW CONCEPTS AND DESIGNS WITHIN THE DLT DOMAIN.

We are in this domain because we recognise the real-world potential of DLTs, but we also acknowledge its current shortcomings and inefficiencies.

We had to build Aleph, because we realised that the current technology was not able to bring our own – or others' – ideas to fruition.

Therefore, we first had to solve the existing industry challenges that are obstructing our own ambitions to build decentralized solutions that are able to solve real-world problems.

The Post-Blockchain Protocol

THE MAJOR TECHNOLOGIES IN THE DLT SPHERE ARE BLOCKCHAINS AND DAGS.

A blockchain is a chain of blocks where each block contains a hash or a unique identifier of the previous one. A block is a collection of data, and each piece of data is added to the blockchain by connecting one block after another in chronological order. A blockchain resembles a flow chart where all points are headed in one direction. In its topological ordering, the sequence flows chronologically. Although in applications the chronological order of transactions in a blockchain is needed at some point, it is not needed immediately.

Blockchains force a total order on transactions simply by adding a new block to the chain. By allowing for a looser structure of how to represent transactions, a DAG relieves the bottleneck of imposing order before it is needed[1,2]. A DAG orders transactions only when they're needed, which improves the efficiency of the system. The transaction time can be a fraction of what it is in blockchains. The different structure of DAGs allows protocols to concurrently process transactions independently.

Some projects are already implementing DAGs as a replacement for blockchains, and DAGs themselves have long been used for solving issues related to data processing, scheduling, finding the best route in navigation, and data compression.

Forbes suggests that DAGs are the next natural step for the industry[3]; however, implementing DAGs alone is not enough to ensure widespread adoption. Even DAGs need to be elevated to the next level because they lack true decentralization solutions. Aleph imposes total ordering on all transactions with the Aleph consensus protocol which greatly improves efficiency.

1 https://stackoverflow.com/questions/2283757/can-someone-explain-in-simple-terms-to-me-what-a-directed-acyclic-graph-i s

2 https://en.wikipedia.org/wiki/Directed_acyclic_graph

3 https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#4fa fc5f0180b

Industry Challenges

TO UNDERSTAND ALEPH ZERO'S VALUE, WE MUST EXPLAIN IN DETAIL THE INDUSTRY SPECIFIC CHALLENGES THAT NEED TO BE SOLVED BEFORE THE INDUSTRY CAN MAKE TRULY GROUNDBREAKING PRODUCTS. COMMONLY REFERRED TO AS THE "BLOCKCHAIN TRILEMMA"[4] (SECURITY, SCALABILITY, AND DECENTRALIZATION), THESE CHALLENGES ARE GENERALLY ASSOCIATED WITH:

<PRIVACY>

<SECURITY>

<SCALABILITY>

<SPEED>

<COST>

4 https://www.coinbureau.com/analysis/solving-blockchain-trilemma/

/ The Privacy Challenge

Current internet policies have turned all of us into data commodities that are up for sale to the highest bidder. It is one of the gravest challenges facing the contemporary internet with many voices demanding that control be put back into the hands of the user.

Blockchain technology is poised to answer these calls with security measures that guarantee utmost privacy with social accountability. Zero-knowledge proofs (ZK-SNARKs) and Secure Multiparty Computation (sMPC) are two of the technologies that can revolutionize the way we perceive internet privacy and help us regain control over the personas we create online.

ZK-SNARKs pass a secure and secret key between users, whereas sMPCs secure data through multiple computers which cannot access data without unanimous consensus. Both solutions will allow the internet to become a place where our sensitive data is released only with our approval.

/ The Security Challenge

Although distributed ledger technologies are considered – by the general public – as almost immune to attacks thanks to their decentralization, evidence speaks otherwise. While Bitcoin might be regarded as relatively safe due to its size, smaller networks are being attacked on a daily basis.

One primary challenge of the majority of current DLTs lies with analyzing the security of their chosen consensus protocol. Due to the longest chain rule, blockchains will never reach finality with 100% certainty about the current state of their ledger. As more blocks are appended to the chain over time, old transactions included deeper in the chain have a higher probability of withstanding a double spending attack. In the original Bitcoin whitepaper, Satoshi considered 6 blocks as a standard to provide enough validation, but this can never be 100%. This means that complete certainty of approved updates does not exist in such algorithms and may allow attackers – in theory – to perform a successful double spend attack.

Taking over 51% of the network's computational power allows the initiation of a 51% attack. If successful, transactions that occurred after the attack was launched may be deemed invalid or not included in the new "longest chain". This is one way a double spend may be achieved by attackers.

Most of the consensus models based on proof-of-stake are vulnerable to denial-of-service (DoS) attacks. This vulnerability is due to being leader-based, at least in some sense. Even if leaders are randomly picked and changed in a round-robin manner, a well-timed attack can be targeted at the network, and bringing down only a few validators at the same time can stop the whole network.

Even if certain types of attacks have not been launched, the theoretical security vulnerabilities of blockchain are still important to understand when using the network. Because of these lack of proofs and theoretical guarantees, such consensus models in the long term do not appear to be practical solutions for distributed ledger technologies.

/ The Scalability Challenge

The early iterations of the technology in the blockchain space do not solve the scalability challenge well in a non-permissioned environment. It is widely known that Bitcoin and Ethereum are limited by scalability issues. With 3 to 15 transactions per second (TX/s), the technology is nowhere near PayPal (average 193 TX/s) or Visa (65,000 transaction messages per second as of August 2017)[5].

Furthermore, the estimated confirmation times for a transaction to be approved by the network in a blockchain can vary from 1 minute to 60 minutes. As observed in the Analysis of the Blockchain Protocol in Asynchronous Networks[6] paper, in every blockchain protocol there is a trade-off between speed and security.

There are protocols that are – in theory – much faster than Visa or MasterCard. The only downside is that they do so in a private, closed environments. If we are debating whether cryptocurrencies can be used world-wide as a standard payment system, we need to build them utilizing a true decentralized fashion.

/ The Speed Challenge

Traditional Bitcoin confirmations can take 10 minutes to confirm, and depending on the load of the network, they can even take up to 40 minutes, which makes it impractical to use for small, quick purchases like coffee. Projects have jeopardized decentralization in order to increase speed, and while faster confirmations are indeed achieved, the resulting increased centralization can be detrimental. DLTs should stay as decentralized as possible in order to provide

5 https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

6 https://eprint.iacr.org/2016/454.pdf

a level of security that can be trusted. Otherwise, they can be manipulated by malicious actions – and that's not what should be exchanged for speed.

Ethereum is much faster than Bitcoin. The transactions only take 15 seconds to confirm, but there is a strict limitation of 15–20 transactions per second, which is still not comparable to Visa or MasterCard, and all transfers require fees.

/ The Cost Challenge

Traditional blockchain protocols require special purpose mining rigs to solve computationally intensive, but easy to verify, mathematical problems. The Bitcoin network is an example of how inefficient proof-of-work-based blockchains can be at scale. Since the computational power in the network increases over time, the difficulty of the mathematical puzzle to solve adjusts accordingly and dynamically. Therefore, the network requires more power, causing high energy consumption and expensive hardware that may have a short lifespan[7, 8]. This also makes mining operations out of reach for the average user due to capital requirements.

ALEPH ZERO SOLVES THESE CHALLENGES

We believe Aleph Zero is the most innovative protocol in the business and that our algorithm is unmatched in sophistication. Aleph Zero solves the aforementioned challenges that prevented other technologies from becoming widely used, even if they were widely known.

To learn more about how we solve industry challenges, and to further explore our ideas and the solutions we introduced in Aleph Zero, please read our platform paper that will be available later this year.

7 https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

8 https://captainaltcoin.com/how-long-to-mine-one-bitcoin/

Use Cases

BOTH DLT AND SMART CONTRACT SYSTEMS PROVIDE EXCEPTIONAL VALUE PROPOSITIONS, NOTABLY REGARDING GOVERNANCE OF THE COMPLICATED MIXTURE OF ASSETS, DATA, AND EQUITY THAT HAS BECOME PART OF EVERYDAY LIFE IN A MODERN SOCIETY.

The functionalities and performance that people expect for the management of their own assets and data in a decentralized environment are growing faster than the systems that currently support them. New systems need to be built to provide the features and interoperability that people expect to be available in the future. DLT and smart contract systems could be the answer to a lot of the use cases that we have, like equity and securities, real estate, and intellectual property.

In this section, we present practical use cases for the Aleph Zero protocol.

/ Internet of Things (IoT)

The IoT sector is vast and diverse. This technology shares data constantly in order to operate. This data is then stored on the provider's servers to improve products or develop user experience. If such a database is centralized, it could be attacked and the data could become compromised. Devices also could be backdoored through a malicious update or receive malicious communications without knowing their validity.

A decentralized protocol for IoT requires a fast and scalable system. IoT has also often been associated with micro-payments, but current systems are cost prohibitive, slow, and centralized.

Unlike current systems, Aleph Zero is fast, highly scalable, secure, decentralized, and allows low-cost value transfer for any size of transaction. Once it is implemented on IoT networks, with an open-sourced community, we can collaboratively contribute to and produce compelling solutions which cater to devices.

/ Smart Contracts

Distributed ledger technology will make a global impact across many industries, increasing efficiency and encouraging collaboration across systems in which entities do not have to trust a third party. Smart contracts open the way for developers to create almost any kind of application, for any business. This is why Aleph is committed to their development.

In Aleph, we are creating fast, secure, and Turing complete smart contracts that will scale for applications that require high computing power. This opens a new world of possibilities for systems with complex machine learning components and other high-scale automated services. In the future, it can allow the deployment of trusted and fully autonomous agents.

It is impossible to predict all of the ways this technology will be used. However, smart contracts running on a decentralized network that provides real-world performance is the best chance of realizing new possibilities.

/ Supply Chain Management

Supply chain management is extremely complex. The process of creating and distributing goods involves payments, invoices, multiple entities responsible for providing services, and thousands of computational decisions across multiple international locations, and it can cost significant capital and time to be custom tailored.

Aleph can solve many problems within supply chains. For example, a currency stored on the Aleph Zero protocol could simplify payments and accounting. The full history of production, logistics, and distribution could be added to the Aleph network, creating a consistently synchronized and fast distributed record that can be trusted.

Everyone would be able to track down the product from the shop shelf, to it's transportation, to the origin of where it was produced. This might incentivize companies to transparently prove they aren't doing things like testing cosmetics on animals or using child labor for their products. An entity could award certificates by verifying vendors' activities.

Additionally, further simplification of supply chains might lead to lower prices of products and improved quality.

/ Virtual Game Assets

Paid extensions and rare items often give a serious advantage to the players who obtain them and can have significant financial value. A theft of such items by hackers lowers the positive gaming experience, reducing trust with in-game purchases.

To prevent such situations, a tokenization system could be created on the basis of the Aleph protocol. It would store the complete history of item ownership and would allow free in-game and out-of-game trading with other cryptocurrencies. A cross-game item exchange could be established to allow players to be able to trade value between the games. This would broaden the options for players to buy in-game items.

Speculation on an item exchange could bring a new forms of rewards for players by exchanging their in-game efforts for other forms of value. For the game developers, it would create new revenue streams, higher engagement, and higher competitiveness. If the game studios will be able to create more value for the players, the whole industry might benefit. Additionally, the tokenization of virtual game assets could bring security and transparency to the gaming industry, especially to multiplayer and casino games, which would also be beneficial for the whole industry for users and developers.

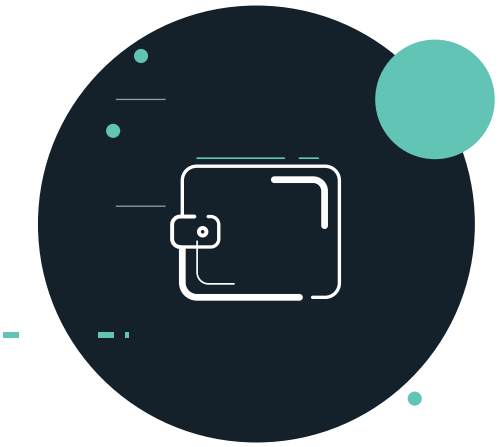
The decentralization of virtual game assets would have to be based on a platform that would not negatively affect the gaming experience. We see Aleph Zero as the best platform to suit these needs; besides its high speed, scalability, and security, its interoperability would enable players to exchange their assets conveniently.

/ Decentralized Domain Name System (DNS)

DNS is what translates domain names into IP addresses. It powers the internet as we know it, and this makes it a potential point of failure. That's why DNS servers are distributed around the globe, but their decentralization is only technical as most of the servers are maintained by large organizations that are influenced by governments and large companies.

Since DNS providers can monitor internet traffic, they can potentially hijack users' internet usage, spy on users and companies, or censor the internet. We have to trust the organizations in control to not perform malicious actions. In this case, we believe it's better to trust math and have provable decentralization than have these risks.

Aleph can become the foundation for a truly decentralized DNS service built into web browsers. This would become the technological trust layer of the internet. It would not allow maliciously altering the end IP address on the DNS side, and it would not need certificates vouching for websites' legitimacy or to encrypt the connection, as it would be a standard. The connection information wouldn't be stored anywhere, improving privacy. It could even speed up the connection, compared to traditional DNS servers.



/ Universal Wallet and Decentralized Exchange

Under development by Cardinal Cryptography

Creating a true universal wallet for cryptocurrencies is one of the major directions of Aleph Zero development.

The problem with many current solutions is that although they are used to store keys for decentralized currencies, they are centralized themselves. This makes them easier to attack or manipulate, and therefore the security of the assets is not guaranteed. That's why we propose a truly decentralized wallet – the Common Wallet – running on the Aleph Zero protocol that can technically operate with any other cryptocurrency, starting from the most popular Bitcoin and Ether to other less popular ones.

Thanks to Aleph Zero being a DAG, the protocol is mining-free, meaning minimal transaction fees. Its decentralized security brings it to the completely trustless level, while the speed of Aleph lets you finally transact with Bitcoin in just a few seconds.

This subsequently allows creating decentralized exchanges for high-scale cryptocurrency trading as well.

You can read more about Common at getcommon.com

/ Asset Digitization

Blockchain technology is seen as a way to simplify many legal processes – such as buying and selling real estate, applying for and receiving a loan, or holding stocks and bonds.

Today, to buy a home – anywhere in the world – apart from the transaction, the buyer and seller need to take care of title management, which involves hiring lawyers and brokers, finding insurance, and so forth. The paperwork complicates the process, but on the other hand, this is the only way to perform these massive transactions while not completely trusting the other party.

Getting a loan for buying a house complicates the process even more. It involves providing documents that could stand as a proof that the one applying is able to return the loan and for what amount.

For stocks and bonds, there might be a need for accreditation, but it also involves receiving dividends and transferring the assets if needed.

Ultimately, looking at these processes on a higher scale, and having a centralized entities to validate the transactions and proofs, exposes the major inefficiency of the current setting. The processes take too many steps and involve too many people for what should be a simple exchange of value.

That's why a decentralized platform like Aleph Zero can make asset exchange and transaction validation much more efficient. It brings security and speed to the process, but at the same time, its smart contracts can be used in the form of "code as law". Therefore, a lot of the paperwork can be completely automated, simplifying the transactions to just "You give me the money – I give you the asset," with a guarantee that everything runs as it should and there's no possibility for manipulation.

But there are still challenges that need to be solved – connecting the real world exchange to the "digital paperwork" done by smart contracts. In this case, there still might be some need for a trusted entity to supervise the processes, but we believe this field can also be revolutionized.

/ Notary Signatory

In the current system, a notary is responsible for witnessing that the sides are willing to sign an agreement with their own will, while being conscious, of sound mind, and so forth. That's why it's still necessary to visit a notary public in order to transfer a title, declare power of attorney, and perform other similar activities.

However, with the technology we already have, it can be done 100% online with a simple video call that would be recorded on a secure, decentralized ledger and stored there as a file, together with the information about the transaction and the identities of the people involved. It could then be accessed at any point in time if any doubt occurs.

Such a solution could eventually replace the need for notary publics, but before it can be achieved, the new system would have to ensure that the transaction and the parties involved are honest. This is a complex problem that could be solved by utilizing Aleph, Image

/ Transparent Public Document Access

Government transparency that enables trust and accountability is one of the pillars of democracy. Such transparency allows media, independent auditors, and regular people to assess the government's actions and, before they are assessed, to discover them. Although some bad actors might hide parts of their activity for political or financial gains, every time such manipulation is disclosed, trust in the government falls rapidly.

The same issues happen too often in business, as well. Dieselgate was one of the most recent examples of such activity. Volkswagen intentionally cheated on laboratory emissions tests and distributed millions of vehicles that far surpassed the limits outlined in the Clean Air Act. When it was exposed, the manufacturer lost trust and had to pay enormous fines. Such activities are usually exposed at some point in time.

In a world where trust is highly valuable, losing it can end up with major revolutions, both in governments and businesses. After all, that's why blockchain emerged. DLTs could impact this area heavily by replacing trust with secure, decentralized platforms.

For example, copyright and patent claims could be easily assessed by data timestamps that can't be altered. It's one of the simplest features of DLT and some entities are already using it. A general transparency might not be suitable for all cases – for example, national security. But there are many areas which might benefit from total or partial transparency.

The Aleph Zero network can be both a public and a private ledger. Therefore, the public network can work as a hub and is suitable for holding the data that can and should be accessible by the general public. Some private chains (the "spokes," as we call them) connected to the public record can enhance the security of other aspects of governing while still operating internally, with access control.

Using Aleph Zero on a public layer can improve efficiency in many areas of governing and business and improve the communication of the two with citizens. Besides the obvious benefit that a decentralized ledger can reduce the amount of paperwork and compliance, it can also bring innovations like algorithmic laws that would be sufficient for emerging technologies, rather than putting them into grey areas as often happens now.

Unless the trust aspect can be handed over to decentralized technology like Aleph Zero, we will continue to witness trust crises for governments and businesses. Only with broadly implemented open data access policies (where needed), we can innovate and legislate faster to grow the global economy.

/ Automatic Tax Payment

Tax payments are fuelling the economy on many levels, but for an average person, they are neither transparent enough nor easy to understand if they have to calculate them themselves. Making a mistake in this area can be very costly, as many have unfortunately discovered.

This is why there is a strong need to simplify and automate this area. At the World Economic Forum in Davos in 2016, 800 attendees took part in a poll on blockchain-based taxes, and 73% of respondents expected that the most developed countries will create blockchain-based tax systems by 2023–2025. It's no longer an 'if'. The government of Estonia has already enabled their e-residents to pay taxes online with their decentralized solution.

Such a system requires a major infrastructure revolution. Just as in Estonia, it would require the provision of a digital layer to the citizens' identities, to know who or what entity is paying the tax, and then have the record of the amount that needs to be paid or that has been paid automatically.

A centralized solution would – most probably – be insufficient. Such a centralized database can be a desired target of hackers, who after breaching the security, could steal identities, create fake ones, or extract information about the incomes of individuals, along with their identities and addresses. A decentralized solution would be much more secure.

With Aleph Zero, the room for tax optimization can still be preserved but the security risk eliminated. With all transactions held on Aleph Zero, and a public ledger and smart contracts enabled on the platform, taxes could be calculated and charged automatically and always correctly. Automatic tax payments could also make cross-border VAT settlements seamless, and with a broad implementation, it could even completely remove the need for accounting, or at least for issuing invoices.

With its scalability, speed, security, and interoperability, Aleph Zero is an ideal solution for creating such an innovative and efficient worldwide-adopted ecosystem.

/ Databases

Data collection has become one of the biggest trends in almost any industry. So-called Big Data is what many business people see as the basis to make well-informed decisions.

The problem is that such big databases are constantly growing in size, collecting lots of data. This leads to overcomplication and makes retrieving actionable insights from the data extremely difficult and time consuming, which makes managing the database inefficient.

Current centralized solutions are fast, and if speed is the priority, no blockchain solution has developed a good alternative, although Aleph is capable of offering similar UX and speed. The centralized databases are permissioned, which usually supports business needs, but require database administrators and other maintenance costs to keep them running. Centralization also means that the system may have a single point of failure, or be the single point of failure.

Not every database should be redesigned as distributed ledger, but migrating them to Aleph Zero could bring much benefit to their owners. A decentralized ledger located on servers in multiple geographic locations is more difficult for cyberterrorists to attack. Additionally, there is no need to consider everything "decentralized" as "public". Aleph is able to run in public or private environments, using the best of these two worlds, while its interoperability allows for a seamless integration of businesses operating on different types of blockchain.

This might bring a great advantage to business partners. A group of companies could share some parts of the Aleph Zero database, gaining efficiency and transparency in their operations. In this setting, the companies wouldn't have to trust each other, and could make better decisions, possibly speeding up their growth.

Blockchain databases are considered inefficient also due to their transaction and mining fees, but as Aleph is completely mining-free, it could lay the foundation for minimal-fee decentralized databases.

Ultimately, Aleph can create a completely new ecosystem that allows businesses to cooperate in new ways, for transparency and higher profits on all sides.

/ Automatic Payments and Shared Revenue Agreement

As Bitcoin is becoming an increasingly valid currency to the general public, it – or any other cryptocurrency that could take its place in the future – could be used to do automatic payments with a set of smart contracts.

Of course this is nothing new, and we are used to it with bank accounts and credit cards – and that's why we have a particular interest in using cryptocurrencies as a development of shared revenue agreements. Revenue sharing models involve taking part in operating profits – or losses – among associated financial actors. This requires the participants to be clear about how the revenue is collected, measured, and distributed. The events that trigger revenue sharing, such as online sales or advertising interactions, and the methods of calculation are not always transparent to everyone involved. Currently, the solution lies in detailed descriptions of the methodology written in the contracts, and the parties in these processes are subject to audits for accuracy assurance.

Aleph Zero could bring transparency and efficiency to revenue sharing models, removing the need for trust or audits. It could simplify the agreements. The parties involved, after discussing the aspects of their cooperation, could use a simple UI that would allow them to create smart contracts for their own purposes. They could generate such a contract for a given period of time and from that point, they would be able to receive mutual benefits without unnecessary additional work.

/ Public or Private? Reasonability of Use Cases

ALTHOUGH MANY BLOCKCHAIN ENTHUSIASTS SEE THIS TECHNOLOGY AS THE ULTIMATE CURE FOR ALMOST ANY PROBLEM, AND MANY PROJECTS WOULD LIKE TO SEE THEIR PROTOCOLS AS HAVING THE POTENTIAL TO BE USED IN ANY CASE, WE PREFER TO THINK ABOUT THE USE CASES OF ALEPH ZERO REASONABLY.

Distributed ledger technologies have many advantages over centralized solutions – they are much more secure and can speed up or automate many processes and paperwork. They have the potential to further shift the economy, bringing back honesty and transparency to businesses and governments. And a permissionless distributed ledger with minimal to no fees such as Aleph Zero is promising for securing IoT networks.

In some cases, however, centralized systems can be faster themselves. If there's not much data to process, decentralizing the architecture just complicates operations. We have also heard concerns from enterprises about their need to keep some data private as it is their competitive advantage that can be worth billions.

That's why we designed Aleph Zero to enable enterprises to use many different solutions that suit various needs but placing Aleph as the interoperating hub, combining these blockchains into one ecosystem. This way, both private and public ledgers could be created to suit more needs. As much as we'd love to say that Aleph is the perfect solution for any use case, we also believe the use of DLT in projects should be well analyzed and tested before their adoption and utilization, and fortunately Aleph does indeed apply to a high number of use cases, offering many opportunities to take advantage of its novel algorithm and technology.

CARDINAL
CRYPTOGRAPHY

Implementation

DISTRIBUTED LEDGER TECHNOLOGIES ARE RELATIVELY NEW. TOO MANY PROJECTS EXIST TO ASSESS EVERY ONE OF THEM IN ORDER TO DEVELOP AN ENTERPRISE SOLUTION ON EACH ONE'S BASIS. THE NUMBER OF PROFESSIONALS – RESEARCHERS AND DEVELOPERS – THAT HAVE EXPERIENCE IN DEVELOPING BLOCKCHAIN IS STILL TOO SMALL. AND IT'S NOT PARTICULARLY EASY TO CREATE YOUR OWN BLOCKCHAIN.

That's why we want to share our experience and knowledge with others. As the Aleph Zero Foundation, we host an incubator for new decentralized businesses that want to develop their own applications.

The Aleph Zero Protocol has been created by an experienced team, Cardinal Cryptography. They are available to provide consulting guidance on developing projects on Aleph Zero, and many businesses can benefit from hiring the team behind one of the most advanced protocols in existence.

As an added value to the services offered, we have entered a partnership with Chainsecurity, an independent company that audits blockchains in terms of their security.

If you would like more information, please contact us – details are also provided on the last page.

Summary

ALEPH ZERO IS ONE OF THE FASTEST, MOST SCALABLE, AND SECURE DECENTRALIZED PLATFORMS. IT OFFERS A NOVEL APPROACH TO MANY PROBLEMS THAT WE BELIEVE HAVEN'T BEEN SOLVED EFFECTIVELY YET.

It can be the foundation of a new economy, bring efficiency to various parts of our lives, and discover completely new ways that businesses, governments, and people communicate.

Most importantly, it's able to act as a hub and spoke, to connect many ledgers, forks, and protocols to operate in one, decentralized ecosystem.

The possibilities are endless.

THE ONLY QUESTION IS:

What are <YOU> going to **build** with ALEPH ZERO?

Team

/ Matthew Niemerg
~ Co-Founder, CEO

Earned a Ph.D. in mathematics in the area of applied algebraic geometry from Colorado State University in 2014. Matthew has held world renowned postdoctoral positions in Korea, China, Canada, and the US. He is a Simons-Berkeley Fellow at the Simons Institute and also a former IBM Center of Excellence Postdoctoral Fellow in high performance computing at Oak Ridge National Laboratory. Matthew has been involved in the blockchain space since 2014 and provides consultation related to security and consensus models, cryptographic schemes, and business development for blockchain-based projects.

/ Antoni Zolciak
~ Co-Founder, COO

Technology marketer with 10 years of professional experience. Involved in various public relations and content creation projects for ING, Samsung, Sony, Olympus, and Nikon. Antoni gained experience at the Corporate Communications department of ABB in Zurich while employed at Admind Agency. Before joining In'saneLab as VP of Marketing, he worked as an inbound marketer for Brand24 and Codewise, the 2nd-fastest growing company in Europe according to The Financial Times, Now, he spends all of his time working for Aleph Zero.

/ Michal Swietek
~ Co-Founder, CPO

Received Ph.D. in pure mathematics for his work in the field of infinite-dimensional geometry of Banach spaces and a Bachelor of computer science – both at Jagiellonian University in Krakow. He has been focused on applying his skills in new technologies such as deep reinforcement learning, machine learning, and neuroscience. Now, he is fully focused on distributed ledger technologies that combine mathematics and computer science in a new way, and he is fascinated by the vast possibilities and potential impact of this emerging field.

/ Adam Gagol
~ Co-Founder, CTO

Wrote a Ph.D. dissertation in mathematics in the area of combinatorics at Maria Curie-Sklodowska University in Lublin, Poland. A beneficiary of a SET project for interdisciplinary research and SSDNM fellowship for mathematical sciences, he has been working for many years as a freelance consultant in the areas of mathematical modeling and machine learning.

/ Pascal Schmidt
~ Board Member

A Swiss national with 10+ years spent working with firms such as Credit Suisse, LeasePlan, Steiner AG, and Calltrade among others. He is an experienced C-level executive with finance and economics expertise, fintech and DLT included. Pascal helps to establish a long-term asset management and investment plan for Aleph Zero.

/ Damian Straszak
~ Senior Developer

Obtained a double major master's degree in mathematics and computer science at the University of Wroclaw. He recently defended his Ph.D. thesis in computer science at École Polytechnique Fédérale de Lausanne (EPFL). The main topics in his research are discrete optimization problems and convex programming. For more than 15 years, Damian has been active in the competitive programming scene. In 2013 and 2014, he advanced to the ACM ICPC World Finals — the World's most prestigious programming competition — first as a participant and then as a team coach. He has been involved in the organization of several large programming competitions.

/ Tomasz Kisielewski
~ Senior Developer

Achieved an MSc in mathematics and a BSc in computer science at Jagiellonian University in Kraków. Fascinated by artificial intelligence, machine learning, and formal reasoning, he is excited to be working with modern and innovative technologies at Aleph to utilize and expand his mathematics and programming skills.

/ Damian Lesniak
~ Researcher

Graduated from Jagiellonian University in Krakow with MSc in theoretical mathematics. A Ph.D. candidate in machine learning, he holds a heavy interest in technology-based drug design. Damian believes that the emerging technologies – especially machine learning and distributed ledger technologies – will influence society the most in the near future.

/ Michal Handzlik
~ Senior Developer

Graduated from Jagiellonian University in Krakow with MSc in theoretical computer science and BSc in theoretical chemistry. He worked as a researcher at several European universities (Jagiellonian University, VU University Amsterdam, Leipzig University) investigating a wide array of topics: category theory, formal languages theory, graph theory, computational quantum physics, and quantum molecular modeling. Over the last few years, he has been involved in the design and development of commercial software for high performance scientific computing.

/ Lukasz Lachowski
~ Senior Developer

Graduated from Jagiellonian University in Kraków with an MSc in computer science, and currently, a Ph.D. candidate in theoretical computer science in the field of computational logic and asymptotic properties of lambda calculus. He worked both as a software engineer and researcher at several large IT companies like IBM, ABB, and SolarWinds. His interest in distributed ledger technologies emerged as a result of recent research in the field of distributed consensus, and thanks to the teaching of the distributed systems class at Jagiellonian University.

/ Joshua J. Bouw
~ Blockchain Developer

Joshua was the receiver of the first-ever smart contract, as one of those involved in the BlackHalo and BitHalo smart contracting platform. One of the godfathers of proof-of-stake, Joshua is a popular speaker on alternative currencies and has represented altcoins at OKCoin and Huboi events. Currently, Joshua is working with the Aleph Zero research and development team to help implement the AlephBFT consensus in Rust.

/ Mateusz Gorecki
~ Creative Director

Marketing expert based in Poland, with over 15 years of experience in design and nearly 10 years of experience in creative direction and team management roles. His career spans the roles of Designer, Art Director, and Creative Director overseeing integrated marketing campaigns across emerging channels, print, digital media, and social media; as well as leading the rebranding and design efforts for large-scale, corporate identity systems. He was most recently the Director of Creative Marketing at Codewise – a provider of AI-powered online ad measurement and management solutions for digital marketers.

/ Aleksander Baczkowski
~ Content Writer

Alex B czkowski is a professional copywriter with an interest in innovative technologies and the arts. His broad resume includes work in film, music, and content production. He now works with Aleph Zero.

/ Paula Damijan
~ Office Manager

With five years of experience in international retail management space, Paula is used to taming chaos and ensuring peace of mind for the team members. Handling most office-related challenges, she's a key element of our passionate organization. Paula holds a Master's Degree in Institutional Consulting and Business Coaching from the University of Silesia.

/ Jakub Kocikowski
~ Scrum Master

Over his 7 years in IT, he gathered both deep technical experience and insight into what makes successful teams. He started working as a web developer, while studying Computer Science at Gda sk University of Technology. He also tried his luck in co-funding a marketplace startup, and worked in the fintech industry for Simcorp. Always striving to improve, and multiply his impact, he realized that the individual excellence can be amplified or entirely blocked by the environment of the team and the organization.
As a Scrum Master, he focuses on creating a learning organization, where business and technology are working together toward common goals.

/ Kirby Ong
~ Community Lead

Kirby has a deep passion for global and macro markets, investing and trading, cryptocurrencies, as well as building passionate communities. Since 2018, Kirby has worked with over 20 cryptocurrency projects, such as Fantom, Celer Network, Algorand, and Energi. Kirby was also the Head of Community at a Singaporean VC and a Community & Growth Manager at hype.partners, a full-service CDA for blockchain companies. At Aleph Zero, he's acting as a Community Lead, helping the team to serve their communities on a variety of platforms.

Advisors

/ Max Torres
~ Advisor

Max has 8 years of financial planning and analysis experience at various tech companies in Silicon Valley. He has managed $800M+ in revenue and 500+ HC budgets while working closely with all levels of the organization. He is a finance professional who is passionate about tech and its positive impact on people's lives. At Aleph, he is our in-house crypto market expert bringing into context the high-level market trends but also managing the day to day financial operations and investor relations.

/ Michael Guzik
~ Advisor

Michael Guzik initiated, built up, and headed Pricewaterhouse Coopers (PwC) blockchain practice in Switzerland for over three years. Afterward, he joined Lykke as a Primary Markets Lead where he pioneered security token and utility token concepts. He also served as a partner with Blockchain Valley Ventures in order to build a new regulated primary and secondary market using smart contracts. He also acted as a Senior Advisor for SIX Digital Exchange. Michael brings significant experience in both the Financial as well as the Consumer Goods industries with a particular focus on regulated DeFi applications and Non-Fungible Tokens for the Consumer Goods Market. Over time, Michael led key ICOs and STOs and pioneered the foundations of digital assets. Nowadays, Michael is a co-founder of KORE Technologies which team offers institutional-grade blockchain infrastructure to corporations—from building, integrating, to hosting trust-critical systems. Partners of KORE include IBM, Phoenix Systems, and Securosys. Michael also invested in Aleph Zero through his investment fund, Dcrypted.

/ Joeri van Geelen
~ Advisor

Business Advisor APAC for the Prysm Group, a New York and Singapore-based economic consulting firm led by Harvard Ph.D. economists specialized in distributed ledger and blockchain technology. Taking a first-principles approach, Prysm Group uses the tools of contract theory, game theory, market design, social choice theory, and monetary economics to design customized solutions for distributed ledger technology and blockchain-based projects. Prysm Group's areas of expertise include consortium governance, consensus governance, token economics, incentive design, and market structure. Prysm Group counts among its Senior Advisors former Chief Economist at Microsoft Dr. Preston McAfee and Nobel Prize winning Harvard economist Prof. Oliver Hart; the firm's research has been presented at DARPA, Federal Reserve, IBM, Microsoft, Pantera Capital, Polychain Capital, a16z, Union Square Ventures, Hashed, Harvard, MIT, NBER, USC, Stanford, and more.

ALEPH ZERO

/ Partners & Investors



ALEPH ZERO

/ Contact Us

alephzero.org

hello@alephzero.org

/AlephZeroFoundation

/AlephZeroFoundation

/Aleph__Zero

/alephzerofoundation

/alephzero

discord.gg/4KAa9H5j2G