

# VELAS

# WHITEPAPER



v1.0

05.03.2021

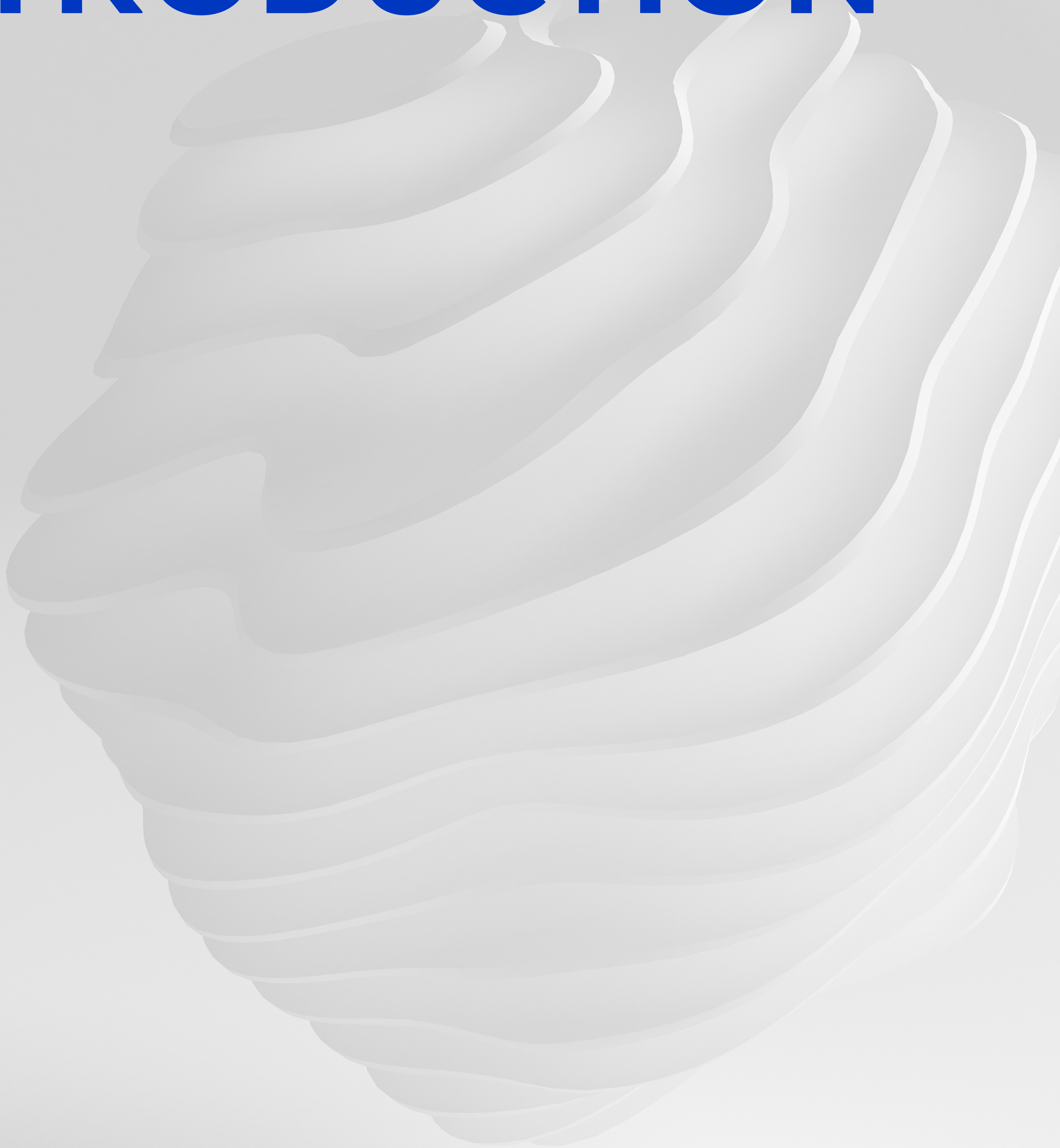
# Abstract

Today, centralized solutions are used everywhere across all areas of our lives. But recently society has started to realize the shortcomings of centralized systems, and how the largest corporations conduct their business. Therefore, we are seeing tremendous growth in decentralized solutions that have emerged thanks to blockchain technologies. Unfortunately, decentralized solutions can hardly be called convenient and user-friendly, which is crucial to reaching mass distribution. Velas want to change that.

This paper contains a description of the Velas Network Ecosystem. Our team has developed a set of technologies that are designed to form the basis for the decentralized Internet - Web 3.0. We took the most useful and applicable technological innovations and built decentralized products based on top of them. We designed our products to be user-friendly, accessible, and as understandable as centralized products, but without exploiting users' data or creating a single centralized point of authority or failure.

With such a mixture, we hope to show the general public all the benefits of using decentralized solutions with Velas.

# INTRODUCTION



## Society

The world has changed fundamentally in the past few challenging years. Unprecedented global events have prompted countless questions to what we should expect next, and how we should move forward. COVID-19 contributed to the increase in speed, growth, and complexity of our society's evolution. Businesses, governments, and private households were forced to adopt digital technologies to reduce human contact. Trends like home workspaces, social media, e-commerce, and online meetings have significantly increased the demand for digital solutions – and that trend won't end once the pandemic is over.

The world has moved into the digital age with the emergence of services and applications that leverage the way we communicate, and transfer information to the next level. The accelerated and forced digital transformation has triggered the need for a constant search for innovation.

The darker side of rapid digitalization has seen the emergence of giants and monopolies, who spread centralization, censorship, and control in and across the digital space and social networks. If you are using popular social media platforms, then your confidential information no longer belongs to you. A large span of companies manage all your personal data for their own purposes. And these problems are the lasting legacy of Web 2.0.

## Web 3.0

People's desire to regain freedom, privacy, and control over their data has led to the emergence of the concept of Web 3.0 – the decentralization of the Internet. It can become true with the advancement of blockchain technology, which has transformed entire industries in recent years.

Web 3.0 will completely erase the boundaries between online and offline, it will be completely authentic and saturated with decentralized applications distributed across domain-specific clusters. The ordered chaos created by the small activities of billions of people is likely to make individuals, companies, and technologies work differently. Work better.

# Blockchain

Blockchain has the potential to revolutionize economic and social interactions, and ultimately become the backbone of a digital society.

Blockchain is a distributed ledger technology that is designed to protect against unauthorized access and ensures that records are immutable (nothing can be erased once it's added) and traceable without the need for centralized management.

Such architecture allows different organizations to utilize one common database, which does not require human efforts to verify the integrity of the data, and is protected from unauthorized interference.

Blockchain technology has proven its capabilities in handling data in a decentralized and secure way, collecting separate fragments into one common whole. Where the internet transmits information, blockchain is capable of efficiently transmitting value, whether it is rights of ownership, goods, or services. Efficiency implies both the speed of information exchange on the blockchain and ensuring its reliability, immutability, as well as building a secure and transparent mode of access to this data by only those who have the right to access it.

This is especially important when the costs of adding data sources and the associated liabilities outweigh the benefits. With the explosive growth in the use of customer data in emerging technologies, such as AI and IoT, visibility is becoming extremely relevant to customers. If the blockchain itself has reached a certain threshold of maturity, then the UX / UI technologies that support it are in their infancy. Soon, they will start a conflict very similar to the conflicts of standards that have led to today's Internet standards. According to Gartner, by 2024, 30% of the sensitive personal data of customers will be protected by licenses based on blockchain technology.

# Velas

Inspired by the values of Web 3.0 and Blockchain technology, we created Velas, a project that combines Blockchain and innovative technologies to create a transparent, community-driven, and decentralized ecosystem of products and services.

Realizing social needs and aiming to become the industry standard, Velas is designed to be a blockchain platform suitable for thousands of applications and services to be built upon. Therefore, we architect it to be one of the most secure and fastest platforms in the industry.


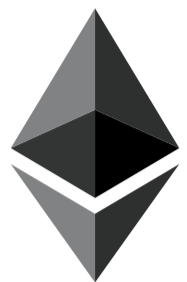

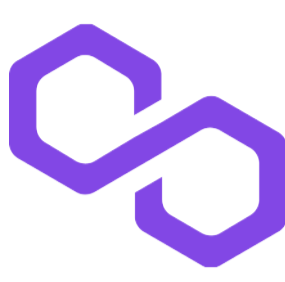
Our mission is to create and integrate world-changing technology products and services to improve people's lives all over the world and make the internet free again - like it was before. We believe that disruptive technologies and innovations will help us to build a self-governed, decentralized future driven by the collective intelligence of the community.

Each of Velas' services is primarily focused on our users. We are trying to combine the best qualities of both centralized and decentralized solutions. It involves researching state-of-the-art cryptography, developing consensus protocols, and designing intuitive user interfaces providing developers, enterprises, and people worldwide to create and join easily accessible, transparent, and community-governed ecosystems for Web 3.0.

To address the main blockchain trilemma, our technologies are being developed with an emphasis on scalability, security, and decentralization.

Currently, Velas Blockchain's performance is much higher than what can be seen across most of the existing blockchain platforms.

## Comparison with others

|                        | <br>VELAS | <br>ethereum | <br>BINANCE | <br>polygon |
|------------------------|--|--|--|--|
| Transaction Throughput | Up to 75 000 Transactions per Second   | ~1000-5000 Transactions per Second   | ~160 Transactions per Second   | Up to 7000 Transactions per Second   |
| Transaction Fee        | \$0.00001  | ~\$6   | \$0.15   | ~\$0.000169  |
| Transaction Finality   | 1.2 sec  | 6 mins (32 blocks)   | 75 sec   | 30 mins to 1.5+ hours  |

To resolve the scalability issue, we've built our solution based on Solana complementing it with additional features and innovations.

Moreover, Velas is a community-driven project. At any time our community members can [vote](#) for the next product our team will place a priority on. This feature and the fact that anyone can join our network as a validator or delegator - makes both Velas and Velas Blockchain decentralized by nature.

# TECHNOLOGY





# VELAS BLOCKCHAIN

Before creating the project idea, the Velas team researched a huge variety of different technologies. We came to the conclusion that the project should solve fundamental problems of both users and blockchain technology in general, and with the maximum achievement of the theoretical performance limit, without compromising on safety and decentralization. That's why we are applying all possible optimizations and innovations at this stage.

We have chosen Solana as a foundation for the Velas Blockchain and complemented it with several innovations to ensure a more secure and user-friendly interaction with our Platform.

Furthermore, we would like to describe the set of technologies that unite together to make Velas Blockchain one of the most scalable, secure, decentralized, and user-friendly blockchain platforms on the market.



## Velas Account

Velas provides its own passwordless authentication system, allowing users to securely access a variety of services without a password using just their Velas Account, while introducing unique authorization quotas to minimize risks.

## Ethereum Virtual Machine (EVM) Compatability

The predecessor of Solana, Ethereum, developed the concept of developer-friendly smart contracts that allows for the realization of all the possible uses with more thought about the process of decentralizing the subject domain and less focus on the limitations of the blockchain.

This enabled many developers around the world to develop a huge number of decentralized Ethereum applications in a short time, some of which even formed ERC standards that became widespread. However, there is no exact reason available why we need to replace this standard with another.

Despite this, developers faced the high cost of transactions, and limited performance of the Ethereum network, which motivated the creation of a more productive Ethereum 2.0.

Ethereum is by far the most widely used DeFi platform on the market, with the majority of dApps built on the network, so this EVM bridge will allow for those applications to run faster and smoother with Velas' increased transaction per second (TPS) capabilities.

Our idea involves a different approach, which is being realized by the Velas team. We take the most efficient blockchain and implement the ability to write Ethereum smart contracts in it, namely the Ethereum VM.

This will open doors for the DeFi market and developers of decentralized Ethereum applications, allowing them to expand their capabilities with the Velas ecosystem, fast Velas blockchain, and low fees.

## Based on Solana

It is highly important to have almost instant confirmation for e-payments. Solana has that.

As all know, blockchain technology is greatly suitable for making e-payments, without the need for a centralized third party to confirm the transfer of funds. When a transaction is confirmed, the nodes (network participants) add information about it to the blockchain.

To reach consensus and legitimize a transaction, blockchain nodes must exchange information about the state of the network or correct to say - synchronize. Synchronizing nodes in the network is one of the fundamental problems of blockchain technology because nodes are located all over the world and have different data throughput capabilities. Synchronization duration proportionally affects the ability of the blockchain to pass more accepted transactions per second (TPS). For example, the bandwidth of the Bitcoin network is 7 TPS, EOS has about 4000 TPS, but the most popular centralized payment system Visa processes around 1700 TPS and dwarfs (with such capability) most decentralized networks.

During our testing of Solana for a full network load, bandwidth reached ~60,000 TPS, and this is not the limit - in theory, it can reach 710,000 TPS on the standard gigabyte network.

Currently achievable performance metrics:

- 59,490 Transactions per Second
- 400ms Block times
- \$0.00001 fee per transaction

How is this possible?

Velas' team understands all outlooks of Solana's approach, and now it's your turn to view these perspectives.

We noticed Solana as the best one-shard chain with vast optimizations within it. The traditional blockchain sharding concept is technically bulky and has additional difficulties.

Solana blockchain can reach a speed of 60,000 transactions per second through GPU utilization, transaction processing parallelization, and other innovations such as PoH and Golfstream. The presence of such technologies in the framework significantly raises the bar for competitors and we consider this framework to be the best solution on the market. Therefore, we chose to use these developments instead of developing competing solutions. Which, in turn, allowed us to fully concentrate on developing the rest of our ecosystem.

The Solana Team composes pioneering technologists from Qualcomm, Intel, Netscape, and Google – and has focused on building the tech required for Solana to function with groundbreaking performance standards.

The main technologies that make Solana so productive and efficient compared to other blockchains are:

- [Proof of History \(POH\)](#) – a clock before consensus;

- [Tower BFT](#) – a PoH-optimized version of PBFT;
- [Turbine](#) – a block propagation protocol;
- [Gulf Stream](#) – Mempool-less transaction forwarding protocol;
- [Sealevel](#) – Parallel smart contracts run-time;
- [Pipelining](#) – a Transaction Processing Unit for validation optimization
- [Cloudbreak](#) – Horizontally-Scaled Accounts Database
- [Archivers](#) – Distributed ledger storage

But, the way Solana optimizes the blockchain affects how developers build decentralized applications on it. They need to think about how the blockchain is structured and develop directly for the Solana blockchain, given all the imposed limitations associated with parallel processing.

## Velas Vault

This is a new technology that allows us to accelerate and cheapen transactions from other cryptocurrency systems by leveraging the speed and security of our blockchain. In this way, we can achieve true security for a decentralized custodian. As an additional perk, we can utilize different authentication solutions, such as Google or Apple Authentication and our own Velas Account, to make the experience of using cryptocurrencies as user-friendly as with all the digital products we use every day. And to add to the number of use cases, our technology can be used to store any data you want in a distributed manner, which completely secures its privacy. And the list of possible applications goes on...

## Velas Freedom

Users don't need to pay when centralized apps perform reads and writes to databases on the backend. Neither should they pay for it on-chain. Building your project on Velas, users may not even realize they're utilizing blockchain services, as transactions are performed on back-end processes.

You maintain the possibility to charge fees in your project's token, automatically and seamlessly in a way that doesn't break the user's experiences.



# VELAS ACCOUNT

According to research by NordPass, the average user holds 70-80 passwords. That is a lot of passwords to remember. It is no surprise, then, that digital users' security is a bottleneck and the main goal of hackers. The FBI Internet Crime Complaint Center estimated that the sheer mass of password-related complaints they received in 2019 alone costs organizations \$2.1 billion.

On the other hand, Internet commerce is growing quickly and experts [predict](#) that it could reach 27 trillion USD by the end of 2027, where payment method convenience plays a major role to outperform the competition.

This is why next-gen authentication and payment solutions become more and more popular as a measure to improve user experience and security.

Having to create multiple accounts across multiple applications and platforms negatively impacts a product's attractiveness and convenience to their user base. Having one Facebook account, for example, enables users to seamlessly sign into other services with it, reducing friction. Paid services, however, request additional information such as credit card binding which is unavailable during a typical user session facilitated by Facebook or alternative social login solutions.

While a combination of centralized solutions, for example, Facebook for login and PayPal for payments might address the problem. Nevertheless, such a setup has its user experience and security drawbacks. Just to name a few: single points of failure, data collection, lack of ability to adjust to custom use-cases, reliance on email with password and etc.

While Facebook, Google, PayPal, and WeChat are the undisputed leaders in today's markets, the blockchain industry is developing alternatives that focus on greater security, privacy, and durability. These alternatives start to form decentralized ecosystems that contribute to the transformation of the way people would manage their digital identities and perform transactions in the future. However, when it comes to authentication and one-click payments, today's user experience of decentralized apps has a large room for improvement due to the complexities of blockchain technologies.

Let's look at Metamask, one of the top wallet apps in the blockchain industry. It supports integration with any website and allows you to authenticate and execute payments through Metamask Browser Extension and recently a mobile app. However, to make payment in ERC20 tokens, you need to sign and broadcast multiple transactions (Approve, TransferFrom) that contain lots of technical information that average users can barely verify if it matches their intent. It's complicated.

Besides confusing the transaction signing process, the other non-trivial task is to properly manage wallet seed phrases.

These two aspects alone significantly worsen user experience that sometimes results in the [loss of funds](#) and it's not surprising that users would prefer services that make authentication and the payment process more convenient, even at the expense of their own privacy. If blockchain payments want to expand their audiences, it has to approach the level of Google and Apple in terms of user experience. This is where Velas Account is meant to perform its mission.

With Velas Account authentication, interaction with cryptocurrencies are facilitated to the level of centralized technology convenience without sacrificing user privacy and security.

- No passwords, no break-ins. Velas Account uses biometric authentication on the user's device to confirm login requests and transactions.
- Seed phrases are available for advanced users, but newcomers can begin their decentralized journey with their Account backed by a social login without the need to manage private keys directly.
- 360° overview of all connected apps and active sessions across all devices with the ability to terminate sessions and revoke permissions of any app at any time.
- With Velas Account, the transaction confirmation screen is free from technical details, providing only the necessary and verifiable information to the user.
- Sending an ERC-20 token to a dApp doesn't require multiple transactions.
- Stay in control of every transaction performed by Velas Account or whitelist well-known apps to execute app-specific transactions in the background.

As a result of these improvements, the user will not feel any discomfort because of the difficulties of using blockchain technologies. The interface will facilitate easy migration from centralized to decentralized solutions, leaving all technical details under the hood and convenient UX.

# VELAS VAULT

## Motivation

As all decentralization enthusiasts, we admire the cryptocurrencies that are bringing the world of decentralization closer to a level of full-blown normalization. Especially Bitcoin and Ethereum for their monumental contribution to the ideas and the concept of decentralized money and smart contracts. But as ordinary users, we see that these systems suffer from slow and expensive transactions, compared with other cryptocurrency solutions. Yet we still use these systems for their security, proven both by time and cryptography.

But, naturally, we want to make those transactions cheaper and faster, without losing the security provided by these systems. There are a lot of solutions on the market that offer to make your transactions almost instantaneous and free if you transfer your coins into their custody. They do it just by maintaining a centralized ledger of balances of all their users, so a transfer to another user is just a small change in a "spreadsheet", which is very fast and cheap by definition. But there are significant problems with these services.

Let's analyze the most common drawbacks of resorting to such solutions:

- 1.** Transferred control of your assets – service keeps the private keys, which means that if there are some problems with accessing the service, such as employee breach or external security breach, then your private keys are at significant risk of being compromised.
- 2.** Hacking and hacker attacks – there exist almost no exchanges that haven't been subject to attacks or thefts of users' funds in one form or another. If you don't hold your keys personally, you are at risk of someone else gaining access to your assets through a wide variety of means.
- 3.** Changes in service conditions – at any moment, the service can impose restrictions or limits on services, including the deposit/withdrawal of funds from your accounts. Again, if you don't personally hold your keys, you are at increased risk of losing access to them.
- 4.** Account blocking and freezing – upon request of regulatory bodies or police/security services, the custody service may be required to limit user access to the platform and therefore their stored crypto.
- 5.** No anonymity – according to FATF rules, the service must collect user data and provide information to regulators upon request. KYC has its perks, but to many, it is a key factor to avoid.

Most of these drawbacks are fundamentally inherited from the centralized nature of such services. To be more precise, the problem lies in the way they guarantee their security. They build it on their reputation and the licensing from government regulatory bodies. So in other words, their security follows from their compliance to the regulations of centralized authorities. But this is in full contradiction with the core ideas of decentralization. True security can only be proven by time and mathematics.

## Solution

As we described before, our primal goal was to make the fastest and the most secure blockchain one-layer system in the world. At the same time, the basic idea of custody service is that a fast and cheap ledger solution can accelerate and cheapen any other cryptocurrency system. As we've discussed, the main question is about security. So what if we can use our blockchain (decentralized ledger technology) as a ledger for custody?

If we do this, then it should only be done in a decentralized manner. But from the dawn of the cryptocurrency era until a year ago there were no suitable cryptographic solutions for the problem of decentralized custody. Yet the strong desire of the crypto-community for a solution to be found gave sufficient motivation for mathematical teams all around the world to search for new approaches to solve the problem at hand. So now let us find out what was the actual problem.

First, we need to understand that any type of custody cannot exist, if the user still holds the secret keys, that allow transferring the coins in custody. Actually, if any one entity knows the secret key, then it is not true decentralized custody. So we have two implications:

- 1) At least one transaction from a user to the custody should be made in the native Bitcoin system by the ways of a slow and expensive transaction.
- 2) No small group of validators, participating in securing the custody, should be able to restore the secret key.

What other requirements are necessary for a decentralized custodian to work? From properties 1) and 2) follows that we need a special protocol to exist that will allow the validators in the custody system to create a secret key in a distributed manner, where no small group can restore this key. And yet the protocol should allow for the corresponding public key to be made known for the users for the purpose of sending transactions to an address in the system.



This task was not the problem, as described protocols existed in the cryptography world for some time. So now we know that it is possible for the validators to create a secret key and corresponding private key in a truly decentralized way. And users can send their coins to the address that is owned by our custody. After that fast and secure transfers are possible in our blockchain. But instead of changing balances in a "spreadsheet", as we described for the case of centralized custody, it will be done via a smart contract deployed on the Velas chain.

So does it mean that we've achieved our goal? The fastest and cheapest transactions of all cryptocurrencies on the fastest chain! But you've probably spotted that there is yet one unresolved question. While we can make fast transactions inside our chain, and Bitcoins (or others) are in custody, the question of exiting the custody remains. And here we enter the problem that for a decade prevented us all from creating a truly decentralized custodian.

To exit custody, we need to make a transaction from the custodian to the user. But we cannot achieve this just by invoking the protocol for restoring the secret key of the custodian. Because in this scenario every validator will be able to sign a transaction that demands the coins to be transferred to his own address. And one of these transactions can get into the block that will be mined first in the Bitcoin network, instead of the one that should have been signed in the first place. So we can see clearly that we need a way to sign transactions in a distributed manner, without restoring the secret key itself. And to understand why it is a huge problem we need to dive deeper into mathematical details of the underlying protocols.

We will start with basic definitions and slowly will go deeper into the details of the needed protocols. Later we will briefly describe existing solutions, their problems, and motivation for the solution we've picked.

# Mathematical descriptions

## Basic Definitions and Schemes

$\mathbb{Z}_p$  denotes the set of all integers from 0 to  $p - 1$  with operations of addition and multiplication performed modulo  $p$ .  $\mathbb{Z}_p$  will be the set of scalars that will be multiplied by  $G$  – the base point of the [elliptic curve](#) that is used in the digital signature scheme from the considered cryptocurrency network. For example,  $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$  for the case of secp256k1 that is used in ECDSA for Bitcoin and Ethereum systems. But in Solana, a different number  $p$  is used for the curve Ed25519 in EdDSA, and there are other examples too.

So why do we need these scalars (multipliers)? The answer is very simple: in every public-key elliptic curve cryptography scheme, the secret key  $sk$  is just an element of  $\mathbb{Z}_p$ . The corresponding public key is always  $sk * G$ , where, again,  $G$  is the base point of the curve. Now we can move to the signature scheme itself.

For simplicity of arguments, we will only consider the ECDSA used in Bitcoin, Ethereum and others. In this signature scheme, when a user has a secret key  $sk$ , the corresponding public key  $pk$ , a message  $m$  to be signed, coded as an element of  $\mathbb{Z}_p$ , the two protocols for signing and verification are:

### Protocol 1. Sign ( $m, sk, pk$ )

1. Sample a random element  $k \in \mathbb{Z}_p$ .
2. Compute the curve point  $R = k * G$ , and its  $x$ -coordinate  $r_x \pmod{p}$ .
3. Compute the signature  $sig = (m + sk * r_x) * k^{-1} \pmod{p}$ .
4. Publish the pair  $(r_x, sig)$ .

### Protocol 2. Verify ( $r_x, sig, pk, m$ )

1. Compute the curve point  $V = (m * G + r_x * pk) * sig^{-1}$ .
2. Accept the signature if and only if the  $x$ -coordinate of  $V$  matches  $r_x$  modulo  $p$ .

Now we move to the decentralized setting. It will involve  $n$  parties (validators, servers, nodes) that can communicate with each other by the ways of secure channels, meaning that only intended recipients will understand the messages sent. As we've seen, the first task is to create a secret in a decentralized way.

Our goal is to allow any subset of  $t$  of them to sign a message, and at the same time to prevent subsets of  $t - 1$  or less parties from gaining any information about the secret key. This problem is called  $t$ -of- $n$  threshold digital signature. It should be clear that in such a setting  $t$  should represent the supermajority of custodians, and that neither  $sk$  nor  $k$  can be stored in one place (be in the possession of one entity).

## Underlying MPC Protocols

Therefore, important questions of multiparty computations arise, when several parties sign the message (evaluate the expression above) without knowing neither  $sk$  nor  $k$ . The standard technique to resolve this issue is called *secret sharing*. We will explicitly derive the details on the following pages for readers to obtain a deeper understanding of the main principles and common pitfalls in this fascinating but complicated topic.

However, let's first suppose for a second, that we already distributed the additive secret shares  $sk_1, sk_2, \dots, sk_t$  and  $k_1, k_2, \dots, k_t$  of an  $sk$  and  $k$  respectively such that  $sk_1 + sk_2 + \dots + sk_t = sk$  and  $k_1 + k_2 + \dots + k_t = k$ . Would it help us sign the document via the aforementioned protocol? We can easily compute  $R = R_1 + R_2 + \dots + R_t$ , where  $R_i = k_i * G$  for the signing phase, and  $pk = pk_1 + pk_2 + \dots + pk_n$ , where  $pk_i = sk_i * G$  for the verification phase, but how do we proceed with the computation of  $sig$  itself?

If you take one more look at the main formula

$$sig = (m + sk * r_x) * k^{-1} \pmod{p},$$

you may notice that it takes more to sign a message because the signature formula involves multiplication by modular inverse of  $k$ , and there is no way to get shares of an inverse from additive shares of  $k$  without revealing  $k$  itself.

We would therefore like to generate the shares of  $k$  in some specific way that will allow us to obtain the secret shares of  $k^{-1}$  as well. This subproblem is solved by a  $t$ -party inverse-sampling protocol described in greater detail in [Doerner et al.](#)

Once we do have such shares  $sk_1, sk_2, \dots, sk_t, k_1, k_2, \dots, k_t$  and  $v_1, v_2, \dots, v_t$  that  $sk_1 + sk_2 + \dots + sk_t = sk, k_1 + k_2 + \dots + k_t = k$  and  $v_1 + v_2 + \dots + v_t = k$ , we can compute the shares  $sig_1, sig_2, \dots, sig_t$  of a signature as  $sig_i = v_i * m + w_i * r_x$ , where  $w_1, w_2, \dots, w_t$  are the shares of  $sk * k^{-1}$ , computed by yet another supplementary protocol for multiparty multiplication. The signature is then restored as  $sig = sig_1 + sig_2 + \dots + sig_t$ .

Now that the main concept is clear, we'll delve into the details.

The first important question is how to distribute shares of the secret key between nodes in a decentralized custodian system. One of the best ways to do this is to use polynomial secret sharing, or as it is better known, Shamir Secret Sharing Scheme.

In this scheme, nodes have assigned addresses  $i_1, i_2, \dots, i_n$ , which are some elements of  $\mathbb{Z}_p$ . To make a  $t$ -of- $n$  threshold secret sharing of secret element  $sk$  from  $\mathbb{Z}_p$ , we randomly pick  $t - 1$  field elements  $c_1, c_2, \dots, c_{t-1}$  from  $\mathbb{Z}_p$  and use them as coefficients of a polynomial  $P_{sk}(x) = sk + c_1 * x + c_2 * x^2 + \dots + c_{t-1} * x^{t-1}$  of degree  $t - 1$  with the free term equal to  $sk$ . After that we create  $n$  shares for our scheme:  $(i_1, P_{sk}(i_1)), (i_2, P_{sk}(i_2)), \dots, (i_n, P_{sk}(i_n))$ . Later another polynomial  $P_k$  is constructed in the same way to distribute the secret shares of  $k$ .

Knowing  $t$  of such shares allows us to restore the secret with a little help from the classical [Lagrange interpolation theorem](#), which states that

$$P_{sk}(x) = \sum_{i \in I} P_{sk}(i) \prod_{j \in I, j \neq i} \frac{x-j}{i-j},$$

where  $I$  is any subset of  $t$  parties from  $\{i_1, i_2, \dots, i_n\}$ .

The current version of the sharing scheme involves a so-called *dealer*, who knows  $sk$  and distributes the shares. It is therefore not suitable for our needs, because we assume that no party (including the user) knows  $sk$ . However, a minor adjustment of the scheme easily addresses this problem. Instead of selecting a polynomial by ourselves, we allow parties to generate their own polynomials  $P_{sk,i}$ , and then define  $P_{sk}$  to be their sum.

The shares are then defined in the same way as before. To compute them, each party  $i$  broadcasts the values  $P_{sk,i}(j)$  for all  $j = i_1, i_2, \dots, i_n$  and learns the values of  $P_{sk,j}(i)$  from all other parties with  $j = i_1, i_2, \dots, i_n$ . Finally, it reconstructs  $P_{sk}(i)$  as the sum of the learned values.

This version is sometimes typically referred to as *Shamir secret sharing with no dealer*.

It is also a basis for widely used [subprotocols](#), such as Biased Random Number Generation (BRNG), Random Zero Generation (RZG), and (unbiased) Random Number

Generation (RNG), which allow multiple parties to generate a common random number in a decentralized fashion.

Note that we never compute  $P_{sk}$  explicitly not to reveal  $sk$ . It is also worth noting that this version is not subject to bias, as the sum of any number of random variables from  $\mathbb{Z}_p$  is uniformly distributed as long as at least one of the variables is uniformly distributed. Note that this statement is the same as the assumption of the absence of  $t$  adversarial parties.

Finally, note that each share is a pair of field elements from  $\mathbb{Z}_p$  and it is only useful in the secret sharing they were created for and gives no information without other shares from its initial creation.

Now that we defined how shares are created, let us describe the details of the above-mentioned multiparty multiplication protocol. For this part, we encourage you to think about  $sk$  and  $k$  in terms of their respective polynomials  $P_{sk}$  and  $P_k$ . To state the problem clearly, we want to multiply  $sk$  and  $k$  without revealing them, using only operations with  $P_{sk}$  and  $P_k$ .

The straightforward way to do this is to multiply the polynomials themselves. The constant terms will then multiply as well. The polynomial multiplication can be easily performed if every party  $i$  multiplies its secret shares of  $sk$  and  $k$ , as  $(P_{sk} * P_k)(i) = P_{sk}(i) * P_k(i)$ . To put it simply, the secret shares of the product are the products of secret shares of the multipliers.

### The Fundamental Problem of Naive MPC Multiplication

However, notice that after we multiply two polynomials of degree  $t - 1$ , the degree of their product is not  $t - 1$ , but  $2t - 2$  instead. One simple example of this is  $x * x = x^2$ , where we get a polynomial of degree 2 from two polynomials of degree 1. In particular, this implies that in order to interpolate the product polynomial we now need  $2t - 1$  honest parties.

Not only does this impose a condition  $2t - 1 \leq n$  or  $t \leq n/2$ , which is clearly not the supermajority we are aiming for, but it also creates the *gap* requirement  $m \leq (n - (2t - 1))/2$  on the number  $m$  of adversarial parties, due to the Reed-Solomon error correction code. These inequalities combined give us a bound of  $t \leq n/6$  for the practical scenario of  $m = n/3$ .

It is possible to avoid the latter bound with [Pedersen commitments](#), but it will not remove the former problem, which has its roots in the naive polynomial multiplication.

This problem is fundamental and prone to the following logical error: one may think that if we need  $2t - 1$  honest nodes to sign the message, then the adversary would also need to corrupt  $2t - 1$  parties in order to forge a signature. This is, however, completely wrong, as the adversary needs not follow the protocol and can simply restore  $sk$  and  $k$  from only  $t$  shares.

This asymmetrical situation feels odd and is not appealing to the public. As a real-life example, imagine having two locks at your door. You need both keys to open it, but everyone else can enter your house with one key only. Sounds weird, right?

The same issue was encountered in [RenVM whitepaper](#), but was not resolved at the time.

However, more recent protocols allow any  $t$  parties to sign while being resistant against an adversary controlling  $t - 1$  parties. We'll summarize some of these here. [Canetti et al.](#) proposed a solution that allows for strong identifiable aborts and fast one-round online signing, removing all the hard computations to the offline stage. [Gennaro et al.](#) also offers identifiable aborts and more efficient computations achieved by limiting the use of zero-knowledge proofs. This protocol also provides a possibility of proactive key refresh (which is especially useful in the presence of cold wallets).

[Ggol et al.](#) proposed what was at the time the first dishonest majority threshold protocol, robust in the signing phase. In [Doerner et al.](#), very few security assumptions are made. However, the number of rounds in the protocol presented in this paper increases logarithmically with  $t$  which might make it slower for larger systems.

After thoughtful consideration of all these protocols, we arrived at the solution that combines their best practical parts. Soon we will publish a follow-up paper describing our approach in greater detail.

# **CONSENSUS MECHANISM & TOKENOMICS**



# CONSENSUS MECHANISM

Before starting the implementation of the Velas Blockchain our team was researching all the possible solutions to find the one that is the most suitable for a decentralized, scalable and secure network with the potential of onboarding billions of users.

To find the solution we have analyzed a total of 48 consensus mechanisms including 34 proof-based, 7 vote-based, and 8 alternatives (DAG-based) solutions.

Having reviewed most of the existing consensus mechanisms, we can summarize that the compute-intensive-based consensus protocols suffer from the issues of high energy consumption, environmental pollution, low transaction throughput, and low scalability.

On the other hand, the capability-based protocols solve the issue of high energy consumption but tend to be biased towards the rich (wealth dominance) and more prone to malicious attacks.

The voting-based protocols solve the issues of high computational energy consumption, low transaction throughput, and scalability in the compute-intensive-based protocols but they make the network less decentralized. Moreover, the number of data transfers is high in voting-based protocols, leading to higher energy consumption.

It should be stated that a need exists for an energy-efficient, decentralized, high transaction throughput, and highly scalable blockchain consensus protocol to address the misalignment between the existing protocols and the customer services where applications are evolving rapidly to meet the requirements of a collaborative large-scale ecosystem.

Therefore, the DPoS consensus mechanism has been chosen as the most appropriate solution that with wise settings could meet all requirements on the network and network participants level:

- It is much more scalable and PoW and traditional PoS consensus
- It is democratic and encourages a decentralized manner of network governance due to the role of delegates in the network
- The entrance threshold in DPoS consensus is extremely low which makes it one of the most decentralized of existing consensus mechanisms
- DPoS mechanisms have strong protection from double-spend attacks.

However, there are a lot of variables in such complex technologies as consensus mechanisms. Thus, the proper setting and correctly established rules of interaction within the network is required.



# TOKENOMICS

## General Overview

Tokenomics are the economic rules of behavior and interaction of participants in the blockchain network. Velas is based on DPoS economics that provides participants with the most favorable conditions for interaction with each other and motivate them to act for the benefit of the network.

Basic VLX metrics:

- Total supply - 2,229,737,314 VLX;
- Circulating Supply - 2,223,461,795 VLX;
- Inflation rate - 8% annually.

Velas has inherited most of the settings designed by Solana. Below you will find documentation related to the parts of Velas' Tokenomics that come from Solana:

- [General Overview](#)
- [Adjusted Staking Yield](#)
- [Terminology](#)
- [Transaction Fees](#)
- [Solana's Proposed Inflation Schedule](#)
- [Storage Rent Economics](#)

## Staking

We have implemented some changes comparing to Solana's tokenomics regarding the amount of tokens participants should have to apply to the particular role:

1. To become a Validator user should have at least 1 mln of VLX Tokens
2. To become a Delegator user should have at least 1 VLX

There are two options for staking in the Velas system – creating your own pool and becoming a [validator](#) or Join an existing pool as a [delegator](#).

DPOS (Delegated Proof of Stake) provides the opportunity for delegators to “vote” on potential validators by staking tokens on them and increasing their chances of becoming validators.