Building dApps at Any Scale

Your starting point to get familiar with the protocol that makes dApp development accessible.

June 2024

verus

Want to build a dApp?

The Verus Protocol offers everything you need to get started *now.*

The origins of Verus.

The first block of the Verus blockchain was mined on May 21, 2018. The chain launch was announced on BitcoinTalk 15 minutes before anyone could start mining, and later staking.

A fair launch with **no ICO**, **no premine** and **no developer tax**. Following into Bitcoin's footsteps as a true, rent-free community project. A necessity to be seen as a credibly neutral protocol for the world.

The vision paper published in June 2018 was the guiding document for the community, its developers and all other contributors.

Thanks to the tens of thousands of miners and stakers around the world securing the protocol, a solid foundation has been built provisioning a truly decentralized blockchain service economy.

After years of development on testnet and various mainnet upgrades, the vision is fully accomplished in October 2023. Verus Public Blockchains as a Service (PBaaS) is now ready to take on the crypto-industry as the protocol for builders.

Everything in this document is live on mainnet, to be used by anyone, completely permissionless. Use these powerful building blocks to create dApps, businesses, economies, systems or organizations at any scale.

The starting point for any serious worldwide protocol is that it has to be credibly neutral.

Click to read:
Verus Vision Paper
PDF

A protocol of unlimited scale.

Verus built a protocol of unlimited scale without sacrificing on decentralization and thus security. While other protocols focus on the 'transactions per second'-metric, Verus offers a different perspective and a new approach.

Verus embraces a multi-chain world—just like the Internet today runs on many many servers.

The key-takeaway here is that the Internet does not run on one single server that is constantly being upgraded to a faster one. This is the equivalent of single-chain protocols boasting about their high transactions per second (tps) throughput. This is what we call scaling up, and sooner or later the single-chain will reach its limits.

The Internet today is a multi-server world, all seamlessly connected. Verus acknowledges this fact, and recognizes that is how the Internet of Value has to scale as well. We call this scaling out. **SEE FIGURE 1.**

An unlimited number of PBaaS-chains can be launched, each with their own organizations or economies needs, completely interoperable, creating a network of unlimited scale.

The Verus blockchain can handle 75 tps. Each PBaaS-chain, depending on its chosen block time, can handle between **75 and 800 tps**.

When a chain gets congested, a new chain is easily started to relieve the pressure. This can only be done when the Verus chain and all PBaaS-chains are fully interoperable, which they are.

All PBaaS-chains (and the Verus blockchain) are protected by the Proof of Power consensus mechanism, a 50/50% hybrid of proof-of-work and proof-of-stake, and provable 51% hash attack resistance. All miners in the ecosystem can merge-mine up to 22 of these PBaaS-chains (including Verus).

Verus scales to any demand by scaling out. Verus is unlimited in scale and ready for any user load.

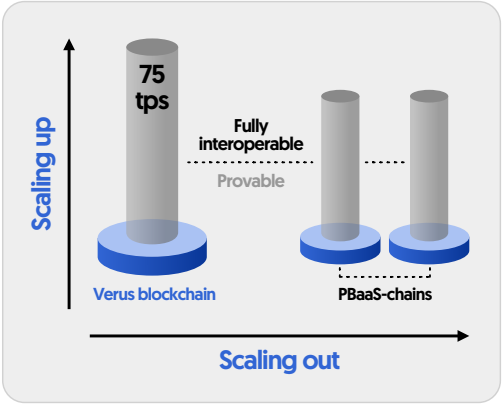

Figure 1: Verus scales out by deploying fully interoperable PBaaS-chains.

Security for all network participants.

Builders and end-users can rely on Verus as a secure protocol. Incredibly important in any decentralized system.

First of all, Verus Proof of Power, the consensus mechanism for Verus and all PBaaS-chains is provable 51% hash attack resistant. Because its a hybrid of proof-of-work and proof-of-stake, it takes a combined effort of a majority of hashing power and staking supply to successfully attack the network.

Secondly, Verus uses 'smart transactions' and not smart contracts. All protocol features are validated and accounted for by the miners and stakers. This means that everything happens transparently and that Verus is not vulnerable to smart contract hacks or bugs.

Because Verus uses smart transactions it doesn't suffer from the insecure and phishing-prone wallet approval mechanisms that are found in VM-protocols. Users know exactly what it is their wallets will execute, unlike other protocols where users often don't know what they give approval for, and can get their wallets drained by malicious actors.

Builders and users can interact with Verus and PBaaS-chains with confidence.

Click to read:
Verus Internet Protocol (VIP) — Provable, Decentralized Cross-chain Communication

Click to read:
A Provable Hybrid Solution to 51% Hash Attacks

PDF

Build low-cost & rent-free.

Verus is a rent-free protocol, not a business. All protocol fees go directly to the miners and stakers. There is no entity that takes a profit or “rent” of any kind.

To build with Verus you don’t need to learn a new programming language. You don’t need expensive Solidity or other blockchain developers. Just build in your favorite framework for clients and access the Verus network either through QR-codes and deep-links to a client-side wallet under user control.

Protocol feature	Details	Protocol fee
PBaaS-chain launch	A PBaaS-chain is a fully independent, interoperable and customizable blockchain. It inherits the exact same features as the Verus blockchain and can set their own prices for VerusIDs & currency launches.	**10,000 VRSC** (5,000 to the miners and stakers of Verus, 5,000 to the miners and stakers of the PBaaS-chain)
VerusID registration	Namespace for currency & PBaaS-chain launches. Or to use as self-sovereign identity or as a controlled public storage system: publish and store data with multiple levels of nesting. E.g. MyBrand@	**20, 40, 60, 80, 100 VRSC** (depending on referrals)
subID registration	Self-sovereign identity for users. Or to use as a controlled public storage system: publish and store data with multiple levels of nesting. E.g. Name.MyBrand@	**0.02 VRSC & defined amount in the currency’s namespace**
Currency launch (e.g. tokens, basket currencies, liquidity pools)	Launch currencies that are backed with or without reserves. Decentralized or with centralized control. Including decentralized crowdfund mechanisms. Or mapped to ERC-20s one-to-one. It is also a namespace to create subIDs.	**200 VRSC**

Protocol feature	Details	Protocol fee
DeFi conversions	Basket currencies and liquidity pools function as AMMs (automated market makers). Verus DeFi is MEV-resistant, low-cost and without smart contract risk.	**0.05%** (for reserve-to-reserve conversions) **0.025%** (for reserve-to-liquidity pool, or vice versa conversions) **50% of the fee goes to the miners and stakers, 50% stays in the reserves**
Verus Storage	A fee-based storage capability for indexed data on the blockchain. All stored data is encrypted by default. All data stored is either sent as part of a private transaction or added to a VerusID (& subID) user's control.	**0.01 VRSC for 1KB** (each PBaaS-chain can specify its own price)

Figure 2: All protocol features and the costs that flow directly to the miners and stakers.

The protocol fees in **FIGURE 2** are for the Verus blockchain. Some of these fees can be changed when launching your own PBaaS-chain.

Additionally to these protocol features that cost fees, each action costs a transaction fee. A transaction typically costs 0.0001 VRSC. Transaction fees are paid in the native currency of the (PBaaS-)chain. Protocol features on different PBaaS-chains are paid in those chain's native currency.

Verus is not a business. All fees go directly to the miners and stakers of the network.

Click to read:
Verus Smart Transactions vs Smart Contracts

Layer-1 privacy.

Verus utilizes privacy technology called zk-SNARKs. It is the industry-leading standard for privacy enabling technology.

The technology is embedded in the protocol layer of the network and can not be seen as an afterthought. Anyone can receive and send untraceable value (the chain's native currency) and data and be private.

It's also possible to exchange data confidentially. Give yourself and your users the confidence to make conscious decisions on what to share, and keep private. After all, privacy is a human right.

Send and receive native assets with zero knowledge privacy

Attach private addresses to VerusID and subID

Store data on-chain, encrypted and private

Share data confidentially

VerusID: self-sovereign identities, namespaces, building blocks.

VerusID is the first decentralized and self-sovereign identity of its kind, the permanent namespace for the Verus Protocol, and the building blocks to create Web3 dApps. VerusIDs (and subIDs) can be created, used and updated with just API commands. Here's a list of its features:

VerusID: **MyBrand@**
subID: **Jane Smith.MyBrand@**

Friendly name address.

Almost all characters from all character sets are available to create a VerusID. Human-readable addresses are the new standard.

Self-sovereign identity.

VerusID can function as a self-sovereign identity for anyone in the world, empowering individuals with complete autonomy both online and offline.

Revoke and recover.

Each VerusID has revocation and recovery authorities. Autonomously revoke access to a VerusID, and recover all assets and data on a VerusID.

Publish & store data.

Use VerusID and VDXF as a controlled public storage system. Publish and store data with multiple levels of nesting.

Verus Vault.

Enable the theft-proof Verus Vault. Set time locks or delayed time locks to secure assets on a VerusID.

Peer-to-peer marketplace.

Exchange peer-to-peer with the decentralized marketplace for VerusIDs, currencies and tokens.

Privacy.

Attach a private address to VerusID. Send and receive native assets with zero knowledge privacy.

Signatures.

Create unforgeable, verifiable signatures with VerusID. Sign files, hashes and messages.

Multisig.

With multi-signature support multiple organizations or people can jointly and securely manage a VerusID.

Messages.

Send and receive completely private messages through VerusID private addresses.

Password-free login.

Login to supported VerusID services without ever needing a password.

SubID support.

Under each launched currency and token subIDs can be registered. SubIDs have the exact same features as VerusIDs (except blockchain and currency launches).

Permanent namespace.

A VerusID/subID is yours forever. No renewal necessary.

Launch PBaaS-blockchains.

Interoperable, independent, customizable, secure.

Launch blockchains for any type of business or organization, inheriting all the same (consensus layer) features of the Verus blockchain. To launch a chain you have to set up witnesses for cross-chain transactions, and just two API commands, one to define the chain and one to launch.

Fully interoperable.

Seamless connectivity between Verus and all PBaaS-blockchains and other connected systems (e.g. Ethereum) through the Verus Internet Protocol (VIP).

Independent.

PBaaS-chains do not depend on or pay rent to any parent chain or system for their ongoing operation.

Customizable.

Define the blockchain specifications and parameters to the specific economy's or organizational needs.

Scalable.

PBaaS-chains have up to 800 tps and can scale out by deploying more interoperable chains.

Shared security.

The worldwide community of miners can mine up to 22 different PBaaS-chains at the same time.

Privacy.

Industry-leading zero-knowledge privacy for confidential exchange of funds and data.

```
./verus definecurrency '{
    "name":"MyBusinessBlockchain",
    "options":264,
    "currencies":["VRSC"],
    "conversions":[1],
    "eras":[
        {
            "reward":1200000000,
            "decay":0,
            "halving":0,
            "eraend":0
        }
    ],
    "notaries":[
        "Notary1@",
        "Notary2@",
        "Notary3@"
    ],
    "minnotariesconfirm":2,
    "nodes":[
        {

"networkaddress":"111.111.111.111:10000",
            "nodeidentity":"Node1@"
        },
        {

"networkaddress":"111.111.111.112:10000",
            "nodeidentity":"Node2@"
        }
    ],
    "gatewayconvertername":"Bridge",
    "gatewayconverterissuance":1000000
    }'
    '{
        "currencies":
["VRSC","PBaaSChain","vETH"],
        "initialcontributions":
[371747.20398827,0,1000000],
        "initialsupply":3000000
    }'

}'
```

VerusID.

Each PBaaS-chain supports an unlimited number of self-sovereign identities (VerusID). These are also the building blocks for dApps.

DeFi.

L1 MEV-resistant, low-fee and no smart contract risk DeFi is supported on each PBaaS-chain. With conversion fees of 0.025% and 0.05%.

Multi-currency.

Each PBaaS-chain supports an unlimited number of currencies, tokens and liquidity pools.

An example of an API command that defines a PBaaS (Public Blockchains as a Service) blockchain. With a specified block emission and a bridge currency that functions as an AMM.

51% hash attack resistant.

50% proof-of-work, 50% proof-of-stake makes each PBaaS-chain provably 51% hash attack resistant.

On-chain economy.

On-chain fees paid to the protocol (chain & currency launches, VerusID registrations, conversion fees and transaction fees) go to the miners and stakers.

Launch any type of currencies.

Tokens, liquidity pools, fractionally backed currencies & more.

Launch currencies with just API commands without any special programming needed. You can use the Verus Protocol for all types of accounting, and communities, businesses or organizations that need a currency.

Currencies & tokens.

From tickets and coupons, to voting cards, meme-tokens, community currencies and for any form of accounting.

Liquidity pools.

Launch liquidity pools with a maximum of 10 currencies in its reserves. With conversion fees as low as 0.025%.

Customizable.

Choose from a large collection of options and parameters to launch currencies and tokens with.

Crowdfunding.

All currencies can optionally be launched through powerful decentralized crowdfund mechanisms.

Bridge to Ethereum.

Bridge currencies, tokens and liquidity pools over to Ethereum as ERC-20, or map ERC-20s one-to-one with Verus currencies.

Secure.

All accounting of all currencies and tokens are verified by block producers. There is no smart contract risk.

Fractionally backed.

Currencies can be fully or fractionally backed—a reserve ratio between 5% and 100%. The reserve ratio defines price volatility.

SubID issuance.

SubIDs are issued in the currency's namespace. Registration fees are defined by the currency launcher and are either burned, or go to the VerusID namespace when it's centralized.

```
./verus definecurrency '{
  "name":"Pure",
  "options":41,
  "currencies":["vrsc","tbtc.veth"],
  "initialsupply":20000,
  "idregistrationfees":0.00021,
  "startblock":2975703,
  "idreferrallevels":1,
  "idimportfees":0.00000001
}'
```

The launch definition of the real-life currency 'Pure'. 100% backed by VRSC & tBTC.

Click to read:
Introducing Pure — The Currency 100% Backed by Verus & Bitcoin

Click to read:
All currency options & parameters. And how to launch currencies.
DOCS

Want to learn more on how currencies and tokens can be used to create real-life value for communities and businesses? Then dive deep with these community written articles:

Click to read:
The Coming of Age of Social Tokens

Click to read:
Community Currencies: A Case Study to Explore New Technical Possibilities

Verus DeFi.

Verus DeFi is truly decentralized and implemented on the protocol level. This has many advantages over protocols that use layer two solutions or even smart contracts.

Low-cost conversions.

A conversion costs a regular transaction fee (0.0001 VRSC or other PBaaS-chain's native currency) + a conversion fee of 0.025% or 0.05%. Half of the conversion fee goes directly to the miners and stakers, the other half is burned into the reserves.

Protocol level security.

All DeFi operations take place on the consensus layer of the protocol, and are verified by miners and stakers. There is no smart contract risk and other advantages:

Increased security at the application level—Verus DeFi is not implemented by having many smart contract authors creating smart contracts on top of the protocol, so there can be no exploits by searching for unintended "cracks" in the seams between contracts.

Increased security at the protocol level—Verus DeFi is implemented in the protocol as part of the consensus, following the fundamental systems design principle which says that the most important security layers should be located in the system/protocol itself.

MEV-resistant.

Because of protocol design there is no front or back running or sandwich attacks. Every participant gets the same, fair conversion rate in one or more blocks.

The Verus protocol solves all transactions simultaneously within a block (as opposed to serially, in order, as is done on Ethereum and all other systems which use the VM-model). This has important implications for security, fairness, and efficiency:

- Elimination of front-running, back-running and sandwich attacks.

- Enhancing system-wide liquidity, thus reducing slippage, as conversions going to and from any given currency within the same block are offset against each other.

- Providing all users converting to and from a currency within the same block the same fair price with no spread.

VDXF: Verus Data Exchange Format.

The Verus Data Exchange Format enables application developers to define globally unique data types and publish references to the same, which may refer to structured or unstructured data that can be located unambiguously via an URL, which implicitly provides both location and

decoding information, enabling applications to use such data, in whole or in part, if they know how, or even ignore parts of the data, while remaining compatible with those parts they understand.

VDXF type keys are globally unique identifiers, which are defined as human readable names along with a specification of how to define and convert unlimited length, human readable type names into collision-free 20 byte IDs, which can be used as type keys associated with content or location values in various forms of data records. These data records, which may have application specific structures or no structure at all, besides length form the basis of an interoperable data exchange format across decentralized applications.

Namespaces for type definitions are equivalent to VerusIDs, a protocol first implemented on the Verus Blockchain, and also one that can support IDs registered on any blockchain or uniquely named system that becomes recognized via a consensus-based bridge on the Verus network. Currently, to be recognized as a unique namespace, the easiest way is to base it on a VerusID, registered on the Verus blockchain network.

Generally, one may think of two types of VerusIDs, those defined on the Verus network or on independent PBaaS-chains spawned originally from and registered on the Verus blockchain network, or VerusIDs, which may also exist on fully external systems that may have been created without any registration on the Verus network initially. In order for an externally created VerusID to be recognizable on the Verus blockchain network or by applications using the VDXF that are compatible with the Verus blockchain network that external system must provide a recognized bridge to the Verus blockchain.

On-chain storage.

With Verus Storage, every PBaaS chain immediately offers a fee-based storage capability for indexed data on the blockchain. Every PBaaS blockchain will have its specific price for storage, ultimately controlled by miners and stakers and defaulting to about 0.01 of the native coin for permanent storage of 1KB of data. All stored data is encrypted by default.

This first version of Verus Storage is great for small to medium size data that you believe is worth storing permanently, as it's limited to a maximum on-chain size of 999,999 bytes. Verus Storage is incredibly versatile, and can be used for VerusID PFPs, HTML content, license agreements, documents. Any information you put on-chain is always available to you anywhere you go, as long as you have an internet connection and your 24-word seed phrase. All data stored is either sent as part of a private transaction or added to an ID you control, using the "data" option.

Data can be easily stored and accessed across all PBaaS blockchains, even in parallel (ie. data sharding) by those with the keys to do so, introducing a market for permanent storage at scale that every PBaaS chain can compete in or price themselves out of, depending on network, project and community goals. Verus Storage capabilities lay a foundation for PBaaS chain projects with economics designed around advanced storage capabilities, applications and markets.

verus

There's only one sustainable way to start building dApps...

Join the community — get familiar, get started.

verus.io/discord

docs.verus.io

wiki.verus.io

medium.com/veruscoin