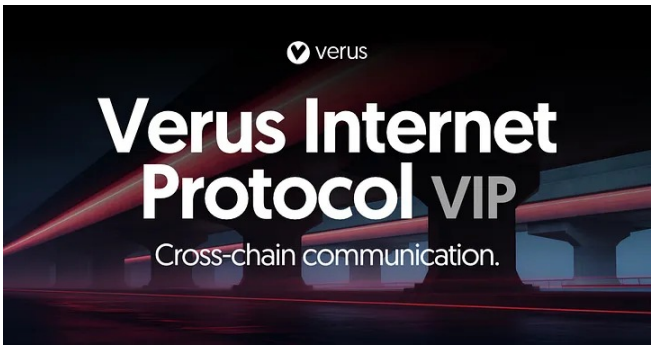
Verus Internet Protocol (VIP) — Provable, Decentralized Cross-chain Communication

Written by Mike Toutonghi, lead developer of the Verus Protocol.

Max Theyse · Follow
Published in Verus Coin · 13 min read · Aug 24, 2023



How it started

Bitcoin proved that decentralized, secure, permissionless and provable agreement on a worldwide blockchain network of participants is possible.

How it's going

companies and app designers, basically writing centralized apps. Instead of a secure set of underlying rules for currencies, we get best practices and the evolutionary legacy of thousands of "dApps", which ironically, are mostly just partial or full re-implementations of the secure primitives missing in the consensus-based L1 protocols themselves.

As a result of the focus on pumping and market capture vs. evolving what we could learn from Bitcoin with sustainable, decentralized, more secure primitives and better protocol design, billions of dollars of value has been lost or transferred from naive early users who bought into the pumped crypto hype to hackers, scammers, VCs, centralized exits, and MEV-exploiters who all leveraged the mass of weaknesses they either failed to protect against or in some cases created and obscured themselves on systems that don't define or enforce even the most common core primitives, currencies or identities. A great deal of loss has been due to obviously poor cross-chain "bridge" design, with the most common problem being bugs in complex smart contract workflow, followed by stolen or compromised private keys of contract owners / controllers, and in some cases, outright

theft by contract controllers.

The lack of agreement on basic primitives and how to represent them in a globally resolvable way has held back general, robust solutions to the fundamental problem of interoperability between blockchains and other financial networks today. To complicate our collective challenges, adding full primitive support in the protocols is hard work, especially in an industry where just a year of development is considered a massive investment that must be rewarded by timely exit liquidity. Consequently, an abundance of shortcuts and heavily marketed yet hastily built solutions still dominate the popular narrative, as hacks, rugpulls, and losses continue to pile up.

The solution

Verus was founded by technology veterans and others who believe humanity can do better than being exploited by the technology these same veterans had been building for corporations over decades. The Verus PBaaS protocol was designed, built, and tested over more than 5 years by a self-selected and often volunteer group of technology, finance, legal, operations, or just life veterans and newbies alike. Early Verusians shared a common vision and made it reality, achieving a fairly launched, community driven project without VCs or ICO participants who may want to exit and a truly decentralized unlimited scale network that all humanity can use and build upon without paying rent to anyone.

It has taken exactly as long as it has to realize the vision laid out 5 years ago, which is more clearly relevant today than ever. Along the way, that vision has grown and evolved as new community members contributed their own vision to help us improve, making the Verus PBaaS protocol, of which VIP is a small part, a major milestone for the crypto industry and a move back to the original intent of decentralized networks that was pioneered, if not fully realized by Satoshi Nakamoto in Bitcoin. Verus has taken Nakamoto consensus to the next level with consensus driven functional protocols for network primitives that are needed in any network hoping to securely enable financial applications.

To ensure maximum decentralization, the Verus Internet Protocol (VIP) takes a maximally decentralized, validator driven approach to its multi-network bridging by incorporating and accounting for currencies, identities, namespaces, and the concept of connected networks themselves in the L0 and L1 consensus protocols. The Verus Internet Protocol provides just enough structure to interoperate with any system that can control funds based on logic and exposes a provable representation of currencies and/or identities.

By grounding interoperability in a cryptographically provable, hierarchical namespace of self-sovereign, worldwide resolvable identities, VIP enables the first high-throughput, unlimited scale, decentralized, multi-protocol, non-custodial, auditable and transparent, currency and identity aware cross-blockchain communications protocol.

A cross-chain protocol with same chain properties

VIP can be seen as a cross-chain protocol that operates on proof of proof of consensus (PoPoC). VIP has the following properties:

1. Transactions that include cross-chain operations, cross-system currency transfers, or new currency and identity definitions, are standardized in the protocol, as are the semantics of their cross-chain use, fee models, cross-system, name-centric provable routing, and MEV-resistant bundling and rollup properties. These characteristics can be and have been implemented on UTXO, VM-based, and transparently centralized networks.
2. VIP supports direct or indirect system<->system communication, including cross-system export and import of currency and identity definitions, as well as revocation, recovery, and controlling keys. All cross-chain or DeFi functions in the protocol are accessible to full or lite node clients and applications by simply creating standard transaction

inputs and outputs that specify the operations. Available APIs on every node or FOSS API server simplify the creation of transactions with cross-chain outputs in response to command requests or JSON RPC calls.

3. Transactions with Identity, DeFi, or cross-chain operations, including all inputs and outputs, even exports and imports of all currencies, are checked for validity by miners and stakers with network consensus, just as single currency inputs and outputs are in today's single currency blockchain networks.
4. Cross-chain protocols operate in the same way as on-chain DeFi protocols and are processed on chain by miners and stakers with a bundle->export->import workflow, enabling high-throughput DeFi and cross-chain operations.
5. In PBaaS, exports, imports, and DeFi operations are all solved simultaneously and processed with at per-block or larger granularity in an MEV-resistant manner as part of the core protocol, recognizing and enabling the need for beneficial arbitrage, while eliminating toxic MEV such as front-running and sandwiching once and for all.
6. All cross-chain operations are proven based on one of the following proof models, which are configurable on a per system/chain basis:

- Decentralized consensus-achieved, witness enhanced, cross-chain cryptographic proofs. (auto-notarization)
- Decentralized consensus-achieved, witness-dependent, cross-chain cryptographic proofs. (notary dependent notarization)
- Semi-centralized or centrally controlled gateway proofs

Full auto-notarization is only available between Verus and PBaaS chains, and operates faster with but is not dependent on notary witnesses. When auto-notarization is applied to other gateway connections, the protocol will fall back to the closest it can come between auto-notarization and notary dependent, which may evolve towards less dependence on the notaries in future versions. Whether you auto-notarize or depend on notary witness confirmation, all forms of notarization operate similarly. We'll start with the basic workflow, then highlight differences:

1. "Earned" and "Accepted" notarizations — VIP broadly defines two types of cross-system notarizations, earned and accepted.

- Generally, one side of a connection will create "earned" notarizations, which on PBaaS chains or for the Ethereum bridge, are created by miners and stakers adding a notarization output to the coinbase. Earned notarizations, which can only be created by Verus or PBaaS chain miners and stakers, include a way to agree or disagree with specific past notarizations, and are subject to further "confirmation" rules, which may vary depending on if the rules are "auto", centralized, or "notary confirm".
- Once a new, earned notarization is confirmed, the proof of confirmation is sent to the "notary" system, which is typically a launch chain, and in the case of the ETH bridge, is Ethereum, along with any notary signatures necessary to prove confirmation, which are typically present. The new, confirmed, earned notarization is entered on the notary chain as an "accepted" notarization, and is entered as "agreeing" with a prior accepted notarization along with proof of the agreement. If the prior accepted notarization it agrees with is not yet confirmed, then it may be considered newly confirmed.

2. Once an earned notarization has been agreed to by a new earned notarization, alternating between PoW and PoS blocks to help further decentralized requirements for agreement, and by following all notarization rules, notary witnesses may sign signifying they agree with the notarization as well. Although they can disagree with a signature, no signature is also a valid way to disagree.

3. After validators and notary witnesses have agreed, or in the case of auto-notarization, a longer validation period with more agreement has passed, the prior notarization agreed with by a new notarization that has passed all necessary agreement, is confirmed. Once that happens, the blockchain is considered final up to the point of that confirmation and will resist reorganizations to any point behind.

The primary difference between notary confirm notarization and auto-notarization is the amount and type of evidence required to enter a potentially confirmed notarization. Most notably, “notary confirm” always requires a quorum of signatures from the specified notaries, whereas auto-notarization requires more multi-stage evidence in the face of randomized proof selection, potential fraud proofs and disagreements. Fully centralized gateways still operate on cryptographic proofs, but they only need notaries to agree on the cryptographic roots in order to consider them true and do not need cryptographic proof to establish the notarization proof root.

Once a proof root has been established by notarization, this root is used to cryptographically prove bundles of transactions exported from one chain or system and imported to another. Even Ethereum transactions are proven in both directions using the same workflow, although Ethereum transactions are validated using PATRICIA Trie proofs, while PBaaS chains use the Verus Merkle Mountain Range (MMR) method, both being cryptographically sound. Cross-chain bundles of transactions follow the same bundling protocol when sourced from Verus or PBaaS chains as is followed in DeFi to prevent MEV.

Transactions are always delivered to the destination network with bundles in the order they were created on the source network and according to the enforceable rules of the source network. Since a relayer may add arbitrage transactions when the destination is a PBaaS chain, but may not affect the provable source contents of a relayed bundle from one network to another, no restriction is placed on who relays a valid bundle of transactions. Since validators who relay and mine or stake transaction bundles into a block may earn a validation fee from the import transaction itself, validators or notaries will generally shuttle transaction bundles between chains and networks out of self interest, while having no ability whatsoever to censor or modify protocol level bundles.

What witness / notaries do NOT do

Witnesses / notaries have no control over what transactions are or are not included or the order in which they arrive from one system to another, as all of that is dictated by the protocol. By default, notaries cannot create notarizations and can only witness the validity of notarizations already created and agreed to by both proof of work and proof of stake validators.

Witness notaries’ primary role is to agree or disagree with the network validators’ earned notarizations, which are earned on one blockchain and accepted on another chain or system. As long as validators enter valid notarizations as part of the merge mining or staking process, confirm other notarizations entered by past validators, and a majority of notaries sign and witness their recognition of those events, a proof root that can be used by anyone to prove committed bundles of cross-chain transactions is established on both systems for the other. As the protocol ensures via cryptographic proof validation that the cross-chain bundles are the exact bundles in the order they were packaged on the source system, importing cross-chain transaction bundles is a permissionless operation that anyone, usually a validator, can perform, which relies on the proof established in relation to a confirmed, notarized proof root.

Do auto-notarization and notary-confirm notarization options have different security considerations?

Yes. Proper planning and selection of options and witness ID structure during the launch of a blockchain network or gateway can ensure that security levels meet network demands. There are security tradeoffs between auto-notarization and notary-confirm options, which basically are a tradeoff between a permissionless model where proof root determination is

enhanced, but not dependent upon multisig agreement of notary witnesses, auto-notarization vs. a model where establishing any cross-network cryptographic proof root requires the honest participation of a majority of the notary witnesses, which can be represented by revocable and recoverable IDs, allowing for further decentralization, even while requiring participation of a quorum.

Determining which option to choose, how many and what notaries to choose, what other safeguards can further enhance security, and then understanding the resulting security profile from each set of choices, is important when launching a blockchain or gateway. The following outlines the current high-level security considerations when configuring a new chain or gateway.

Currently, Verus VIP supports 2 proof models for interchain communication, the Verus PBaaS Merkle Mountain Range proofs, which also assume the Verus Proof of Power protocol, and Ethereum PATRICIA Trie proofs that enable interfacing with VIP between any PBaaS chain, and any Ethereum VM + PATRICIA Trie compatible network.

Since Verus PBaaS is the only interface to fully support notarization finalization using full auto-notarization, it is important to understand the differences between PBaaS and Ethereum proof protocols. At present, there is no objective proof protocol implementation for Ethereum that is known and implemented, which can operate without dependence on some set of notary witnesses. At this time, auto-notarization, when applied to Ethereum, is more similar to notary-confirm, with additional revocation safeguards that could address more edge-case threat models.

As new proof algorithms evolve for Ethereum, enabling trustworthy cross-chain proof models in both directions that are both timely and do not need to be backed by witness signatures, it will be possible to update the protocols to remove dependence on witnesses over time. To ensure maximum decentralization on the Ethereum bridge, the network itself can permissionlessly propose contract upgrades, and if affirmatively voted on by Verus validators, an upgrade and new contracts can eventually change the cross-chain proof conditions.

Auto-notarization of one PBaaS chain on another (PBAAS_AN) differs from and Ethereum interface or notary-confirm (NC) in that, if there are enough validated blocks, both mined and staked, as well as validator agreed notarizations, PBAAS_AN allows validators to finalize a notarization and submit it to the alternate chain. If there are disagreements about the correct notarization, the process becomes an on-chain proof competition, requiring each party to represent a growing, actual chain with both proof of work and proof of stake with an eventual winner. NC still has the miners and stakers create and earn from earned notarizations, but it also must have agreement from specified notaries to finalize any notarization and cannot finalize cross-chain proof roots without that agreement.

Improvement over common cross-chain protocols

Since Verus VIP does not ever have any identity, multisig or otherwise, hold custody over any funds when crossing from one decentralized network to another, even in the context of the Verus Ethereum contracts, threats caused by malicious notaries or stolen keys to drain funds on decentralized bridges or currencies are simply not viable against the Verus VIP protocol.

Cross-chain notarizations must first be entered by an earning validator, either PoW or PoS, and must also be agreed to by another validator, alternating between work and stake in eligibility. Only after that happens can notary witnesses apply their signature and agree to make that a confirmed notarization candidate. Still, what happens if a majority of notaries are malicious and colluding, or if some entity was able to somehow steal a majority of the notary private keys?

If the majority of notary witnesses are honest and operate their witnessing

nodes according to the protocol, the security of such a model should be sufficient for any level of cross-chain transaction proof. If, however, a majority of the notaries were colluding and malicious or if their keys were stolen, Verus VIP still provides ways to ensure that the protocol responds to such a situation without risk of loss. Although there are ways to mitigate such a form of attack, even if no mitigation were available, such malicious or fraudulent notary witnesses would need the following in order to attack a PBaaS cross-chain connection:

1. Colluding, malicious notaries
2. Fake validators with more combined hash + stake power than the publicly validated chain making earned notarizations
3. Developers helping them by creating an alternate protocol for the shadow chain

While you may recognize these requirements as very close to the requirements of attacking any blockchain, the Verus VIP protocol provides a way to even defend against such an unlikely scenario. VIP provides for revocation of all VerusIDs, including notary IDs, even those that are used for Ethereum protocol bridges. Furthermore, each PBaaS chain, including Verus, has a network agreed multisig chain oracle that can separately pause cross-chain notarizations or transactions temporarily, which also can be overridden by network validators.

To enable yet another layer of safeguards, the Verus VIP protocol does not confirm any notarization that has first been agreed to by validators, then agreed to and signed by all notaries on either the earned or the accepted chain, until a second such notarization confirms the first. This ensures that every notarization on any chain is first made public, given a period of time before confirmation, and finally, if nothing stops it, confirmed.

Meanwhile, with basic monitoring by witnesses to see if their own identities have signed for anything they do not actually agree with, meaning their keys were stolen, notaries can auto-revoke their own identities and prevent stolen key attacks from being anything more than an inconvenience. Additional monitoring by chain oracle controllers to look for clear discrepancies between soon to be confirmed notarizations and chains that they monitor can also use the oracle notification network to pause cross-chain transactions, providing yet another line of defense for each chain on the network.

While there are numerous capabilities and safeguards built into the Verus VIP protocol beyond those described in this document, by separating the proof root notarization process and using cryptographic proof as the foundation of a provable, high throughput, cross-chain export/import protocol, **VIP enables the most secure, scalable, decentralized and multi-modal cross-chain protocol ever designed for blockchains and the Internet of Value.**

. . .

Try the Verus Protocol Yourself! ✅

Look up **docs.verus.io** to use many API commands (e.g. **launching currencies, tokens & liquidity pools**).

Or look up the **complete command list here**.

. . .

Join the community. Learn about the protocol. Use Verus & build.

➡️ **Join the community on Discord**

Follow on Twitter

Go to verus.io

Blockchain Technology | Blockchain Development | Crosschain | Cross Platform | Cryptocurrency

142

Written by Max Theyse

149 Followers · Editor for Verus Coin

Follow

More from Max Theyse and Verus Coin

Max Theyse in Verus Coin

Introducing Pure — The Currency 100% Backed by Verus & Bitcoin

Pure is a decentralized currency fully backed by Verus (VRSC) & Bitcoin (tBTC).

8 min read · Mar 16, 2024

196

Max Theyse in Verus Coin

Verus: Profit Generating Protocol for Miners and Stakers

Future and present Verus miners: take notice. Be ready to maximize profit with your...

4 min read · May 12, 2021

304

Oliver in Verus Coin

How to Start CPU Mining Verus Coin VRSC from Your Computer i...

A Dummies Step by Step Guide to Pool Mining Verus Coin with a CPU!

8 min read · Jan 10, 2019

346 1

Max Theyse

How to preconvert into Bridge.vARRR

Participate in the first ever Verus PBaaS-chain launch — vARRR. Learn how to...

4 min read · Mar 20, 2024

259

See all from Max Theyse | See all from Verus Coin

Recommended from Medium

PYRIN-ONE in pyrin

PYRIN AMA (Ask me Anything)

On February 1st, 2024, the PYRIN team held its first AMA (Ask Me Anything). The team...

13 min read · Feb 2, 2024

143

Max Theyse in Verus Coin

How-to Participate in the Verus-Ethereum Bridge Launch

Instructions on how to use the Verus-Ethereum Bridge website and Verus Deskto...

5 min read · Oct 12, 2023

146

Lists

Generative AI Recommended Reading
52 stories · 894 saves

Modern Marketing
103 stories · 523 saves

Perzibal

How to mine TAI using TonAi on telegram ? Full guide.

Start Mining on Telegram bot for Free

2 min read · Feb 11, 2024

4

MXS Games in MXS Games

MXS Games Public Node Licence Sale Is Now LIVE!

In the true spirit of a fair launch, we are happy to announce that we will make a massive 95...

5 min read · Jan 29, 2024

1

Ilya Ermilov

HOT (Near Protocol) Mining and some hints

Hello friends!

8 min read · Feb 19, 2024

41

Albert Peter in Cryptocurrency Scripts

Top 5 Crypto Gems Predicted to Reach 100x-1000x Gains in 2024

Discover the top 5 crypto gems poised for 100x-1000x gains in 2024. Don't miss out on...

6 min read · Mar 14, 2024

538 13

See more recommendations