BOB: The Hybrid L2

Vision Paper, October 2024

Alexei Zamyatin and Dominik Harz
research@gobob.xyz

Abstract

BOB is a new type of Bitcoin-secured blockchain: a Hybrid L2. Hybrid L2s inherit security from Bitcoin, as the most secure and decentralized network. Bitcoin security is then used to create trust-minimized bridges to Bitcoin, Ethereum, and other L1s. As a result, the Hybrid L2 does not rely on third-party bridges for interoperability and solves the problem of fragmented BTC multi-chain liquidity.

1 Introduction

Bitcoin was created as a decentralized, transparent, and censorship-resistant payment system. A decade later, smart contract chains enabled the creation of decentralized financial applications and other innovative products including NFTs, tokenization of social media and gaming, as well as DAOs and other trust-minimized governance structures. Bitcoin, while remaining the centerpiece of global cryptocurrency adoption, has fallen behind in terms of innovation and developer activity.

Despite its slow and rigid nature as a network, Bitcoin remains larger in terms of market capitalization, trading volume, and active users than all other cryptocurrencies combined. With 300 million users globally, a 1 trillion dollar market cap, and unmatched brand recognition, Bitcoin is as dominant as ever. However, it has the least amount of DeFi activity. Compared to Ethereum, where the DeFi TVL to market cap ratio sits at 30%, Bitcoin's DeFi TVL merely amounts to 0.1% of its market size - a 300x discrepancy.

In the past years, numerous attempts have been made to introduce smart contracts and DeFi to Bitcoin through protocol changes and forks, without success. Bitcoin has opposed all protocol upgrades, such as smart contracts, that would substantially change its functionality or introduce complexity. It is fair to conclude that Bitcoin will not have native programmability as we know it from Ethereum any time in the near or distant future. As such, all paths ultimately lead to the establishment of Bitcoin L2s as the go-to solution for BTC DeFi.

Hybrid L2 . This paper introduces the Hybrid L2, a novel Bitcoin layer 2 solution designed to address the key challenges of creating and scaling DeFi on Bitcoin. The Hybrid L2 achieves three key properties:

- **Bitcoin security** achieved through optimistic verification and fault proofs on Bitcoin using BitVM2[4].
- **Trust-minimized BTC bridge**. Using an BitVM-powered bridge design, users can deposit and withdraw BTC to and from BOB as long as Bitcoin is secure and there is at least one honest node in the network (e.g. the users themselves) to perform an on-chain dispute. This new security model is termed existential honesty (1-of-n) and is strictly superior to existing BTC multisig bridges that rely on honest majority assumptions (t-of-n).
- **Trust-minimized bridge to Ethereum**, secured by Bitcoin. BOB combines the bridge design of L1/L2 optimistic Ethereum rollups with a Bitcoin light client encoded as an L1 smart contract, conditioning the correctness of L2 withdrawals on Bitcoin finality. This design can be extended to the majority of L1 chains that have smart contracts.

As the first Hybrid L2, BOB offers a practical solution to the problem of trustless interoperability: Bitcoin, as the single most trusted network, secures both the L2 and all its cross-chain bridges. BOB further solves the challenge of BTC liquidity fragmentation across dozens of chains. Instead of wrapping BTC into DeFi-capable chains, users deposit assets from various chains onto the BOB network to take advantage of native BTC liquidity and Bitcoin-secured withdrawals. Finally, by contributing fees to Bitcoin, BOB contributes to the long-term sustainability of BTC's security budget.

2 Bitcoin L2s Today: Cure and Curse

Bitcoin L2s have the potential to bring innovation back to Bitcoin, without changing its core principles. The promise of unlocking DeFi use cases such as trading, lending, and staking for Bitcoin's trillion-dollar market without the need for centralized exchanges has attracted thousands of developers: dozens of chains already claim the "Bitcoin L2" title.

However, building Bitcoin L2s is hard, and previous attempts have struggled to achieve the same level of traction as their Ethereum counterparts. We consider the following three challenges at the heart of launching a successful Bitcoin L2:

- **Bitcoin security and trust-minimized BTC bridging**. This is what sets Bitcoin L2s apart from all other chains. Security from the most robust and decentralized network paired with a way to deposit and withdraw BTC without trusting any 3rd party. So far, this has not been possible: almost all BTC bridges are trusted multisigs. Only now, for the first time in Bitcoin's history, we finally have a blueprint for achieving this in practice with BitVM2.
- **Building a competitive ecosystem**. An L2 is only as successful as its dApp ecosystem. A cornerstone of creating successful products is the availability of best-in-class developer tooling and DeFi infrastructure, such as wallets, institutional custody, and oracles. This also means keeping up with new developments including sub-second transaction speeds and abstraction of gas tokens. Failure to provide a competitive builder environment makes it almost impossible for Bitcoin applications to compete with their competitors on Ethereum and other networks. As of this writing, the benefits of non-EVM smart contract environments, even when optimized for certain use cases, are generally overshadowed by the lack of infrastructure and the resulting negative impact on the go-to-market timeline of applications.

- **Onboarding bluechip liquidity (cold start problem)**. Liquidity in stablecoins, on/off-ramps, centralized exchange access, and bridges to other networks, as well as power users, is critical for the success of a DeFi ecosystem. Building on chains that operate in isolation introduces major risks for application developers, as network effects have shown to be a decisive factor in the success of new products.

3 Background: Bridges, Light Clients, BitVM

The Hybrid L2 makes use of three main concepts: light clients, bridges and optimistic verification on Bitcoin via BitVM.

Light Clients Blockchain light client protocols, in the case of Bitcoin also referred to as "Simplified Payment Verification" (SPV), allow nodes with limited resources to efficiently verify execution of payments without downloading the entire data of the underlying blockchain. Instead, only block headers, which contain sufficient data to verify consensus finality, and selected transactions are required. The complexity and security of light client protocols is determined by the consensus mechanism of the respective chain. Bitcoin's light client is provably secure and can be easily verified by other chains that have smart contract capabilities, e.g., Threshold has been operating such a light client on Ethereum for multiple years[1]. Ethereum, on the other hand, does not have a secure light client yet due to the complexity of storing and tracking the public keys of over 1 million validators[2].

Bridges Bridging or "wrapping" assets securely across two distinct blockchains has been proven (i) to require both chains to operate correctly and (ii) to be impossible without a trusted third party[5]. However, in practice, we can reduce the trust required in this third party by enabling any network participant to assume this role. This can be achieved by so-called "light client bridges", where two chains A and B are able to verify each other's consensus protocol as part of on-chain smart contracts. When we deposit asset a into the bridge on chain A, a smart contract on chain B verifies that this transaction has been finalized under chain A's consensus before minting the wrapped representation $b(a)$. Vice-versa, when we destroy $b(a)$ on chain B to receive the underlying asset a on chain A, we first verify that this transaction has indeed been finalized on chain B as part of chain A's consensus. As a result, the only trust we require, in addition to the secure operation of both chains, is that there is at least one node that will relay the data necessary to perform the verification between the two networks. Unfortunately, this design has rarely been implemented successfully in practice due to the complexity of light clients. In the case of Bitcoin, the limited expressivity of its scripting language paired with restrictive block and stack size limits, have made it impossible to implement any form of on-chain light client so far.

BitVM BitVM is a mechanism to execute arbitrary programs on Bitcoin in an optimistic manner: the execution happens off-chain but in case of failures, disputes are resolved and enforced on-chain[3]. The two main use cases are Bitcoin optimistic rollups (similar to Arbitrum[2]) and trust-minimized bridges. In both cases, BitVM allows users to deposit and withdraw BTC from an L2, such that the deposits cannot be stolen as long as there is a single honest and online node in the network - enabled by light client verification.

Please refer to our latest paper for a full protocol specification of the BitVM2 protocol as well as a trust-minimized BTC bridge that uses BitVM2 to implement light clients for connected chains[4]. The design can be summarized as follows:

1. Compress a program into a SNARK verifier (e.g. Groth16[1]), implemented in Bitcoin Script.
2. Split the verifier into sub-program chunks, max 4MB each, such that each can be executed in a Bitcoin transaction.
3. The BitVM2 Operators commit to the program during setup using Taproot trees[3] and transaction pre-signing.
4. A user deposits some funds into BitVM2 (e.g., bridge deposit).
5. When attempting to withdraw funds from BitVM2, the Operator can be challenged by anyone (e.g., if the Operator is trying to steal from the bridge).
6. If challenged, the Operator must reveal all intermediary sub-program results, showing how they ended up with their final computation result.
7. If the Operator is cheating, one of the revealed sub-program results will be incorrect. Anyone can then disprove the Operator by executing that specific sub-program in a Bitcoin transaction to produce the correct result as a fault proof.
8. The faulty Operator is kicked out and can no longer access the funds deposited into BitVM2.

4 The BOB Hybrid L2

The Hybrid L2 design builds upon the notion of trust in Bitcoin security paired with its simplicity in terms of consensus verification.

4.1 Bitcoin security

The BOB Hybrid L2 will use Bitcoin for settlement and security. It is widely accepted that the ideal design for Bitcoin L2s are zero-knowledge rollups (zk-rollups), where state changes are computed off-chain and are then proven as valid on-chain using zero-knowledge proofs. As of today, zk-rollups are not yet possible on Bitcoin: efficient implementation of zk-verifiers in Bitcoin Script requires additional op-codes to be introduced via a consensus fork.

As a result, the practical path to achieving Bitcoin security today is through optimistic verification powered by BitVM2. This means implementing a zkVM which produces validity proofs for each state transition, and posting these proofs together with the state difference to the Bitcoin mainchain in regular intervals. When paired with BitVM2, this allows any network participant to challenge and disprove failures via fault proofs. Similar to ETH L2s, the state can be considered finalized if there are no fault proofs during the challenge period, e.g. 7 days. Security is *almost* equivalent to that of Bitcoin: as long as there is one online node in the network to trigger a fault proof.

There exist a number of technical trade-offs between different optimistic roll-up approaches within the BitVM design space, balancing security against efficiency and practicability, including considerations around data availability, permissionless challenging

[1] https://github.com/keep-network/tbtc-v2/blob/main/solidity/contracts/relay/LightRelay.sol

[2] https://github.com/ethereum/annotated-spec/blob/master/altair/sync-protocol.md

[3] https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

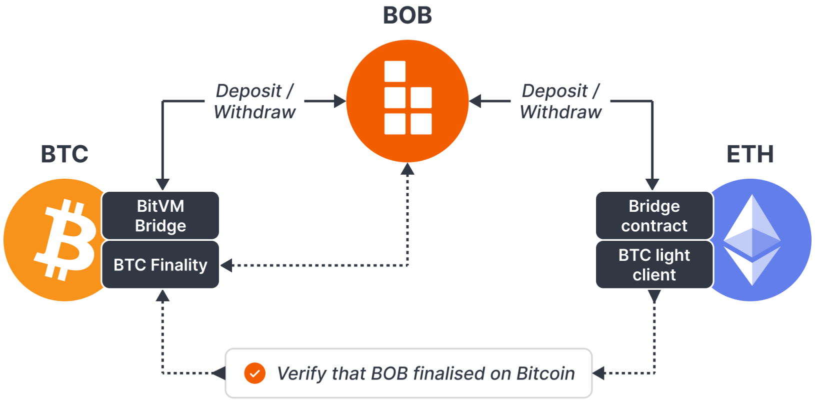

Figure 1: The BOB Hybrid L2 will operate trust-minimized bridges to both Bitcoin (via BitVM) and Ethereum. The Ethereum bridge smart contract verifies that BOB has finalized on Bitcoin using a built-in Bitcoin light client.

logic and light client models. Implementation details for BOB's Hybrid L2 will be found in the forthcoming technical specification.

4.2 Trust-minimized Bitcoin bridge

Optimistic verification via BitVM2 fault proofs also allows BOB to create a trust-minimized BTC bridge. Specifically, a light client bridge where Bitcoin runs a light client for BOB in BitVM2, allowing us to enforce correct bridge withdrawals. Any user that deposits BTC into BOB can be sure that they can withdraw back to Bitcoin as long as Bitcoin is secure and there is one online node in the network to trigger a fault proof.

The security model of the bridge is referred to as *existential honesty*, i.e., it only requires a 1-of-n honesty assumption for correct operation. For comparison: the vast majority of BTC bridges today rely on multisignature schemes and operate an *honest majority* assumption, i.e., t-of-n signers need to be honest such that $t >$ 50%. If the majority of signers are dishonest, they can steal all the funds in the bridge. In contrast, in our BitVM2 bridge design *funds cannot be stolen even if all the bridge operators are dishonest.* As long as there is an online participant, which can be the bridge users themselves, the dishonest operators will be challenged and removed from operation one-by-one. In the worst case scenario, all operators will be removed from the bridge, leaving the funds frozen. This would still constitute an operational failure, with the following subtle but important difference to existing bridge models: operators have zero economic incentive to attempt attacks as they cannot actually steal the BTC. This constitutes the most secure BTC bridge design in the history of Bitcoin.

4.3 Trust-minimized Ethereum bridge

BOB's hybrid design supports secure deposits and withdrawals of ETH and ERC20s. It works similarly to the native Optimism bridge: when users want to withdraw assets back to Ethereum, the bridge smart contract on ETH mainnet waits for the L2 to finalize. For ETH L2s this means waiting for 7 days to make sure there is no fault proof posted to Ethereum mainnet. In BOB's Hybrid L2 design, the ETH bridge smart contract instead waits for BOB to *finalize on Bitcoin*, i.e., ensuring there are no fault proofs posted to Bitcoin. This is achieved through a Bitcoin light client as part of the bridge smart contract that can verify the Bitcoin blockchain. As a result, any user that deposits ETH and ERC20s into BOB can withdraw back to Ethereum as long as Bitcoin is secure and there is one online node in the network to trigger a fault proof *on Bitcoin.*

5 Outlook: BOB as the Center of BTC DeFi

The Hybrid L2 uniquely positions BOB to become the largest DeFi ecosystem, leveraging the network effects of both Bitcoin and Ethereum, and scaling to other chains in the future.

Bootstrapping via Ethereum For dApps on BOB, this means that they can bootstrap via Ethereum's network and benefit from best-in-class infrastructure and tooling, while onboarding DeFi power users and leveraging connections with all exchanges and institutional players. Notably, almost all Ethereum users have BTC and most Bitcoin power-users also use ETH DeFi.

Growth, powered by Bitcoin . With time, the added security from Bitcoin and access to BTC via a trust minimized (BitVM2) bridge, will unlock more and more of the massive pool of so far untapped Bitcoin liquidity, allowing dApps on BOB to not only catch up with their Ethereum competitors but to outgrow and outperform them. This effect is further enhanced by Bitcoin's global adoption and diverse community: while ETH L2s keep fighting for the same user base, BOB dApps can tap into Bitcoin's 300 million global users and thousands of real-world businesses.

Bitcoin as the multi-chain DeFi hub Bitcoin, Ethereum and stablecoins make up 90% of the market. However, just like there exist hundreds of banks, there will likely exist hundreds of chains specializing in different use cases and geographic locations. Their users will need secure access to BTC and a way to exchange assets.

Today, this is the role of centralized exchanges: exchanges connect to all chains, allow users to deposit, trade and then withdraw the assets back to the respective L1. However, centralized exchanges have an expiration date. They have caused major issues in the past and will continue to do so until we fully transition to DeFi.

Instead, BOB's mission is to make Bitcoin the backbone of a secure and transparent DeFi ecosystem. As a Hybrid L2 BOB will

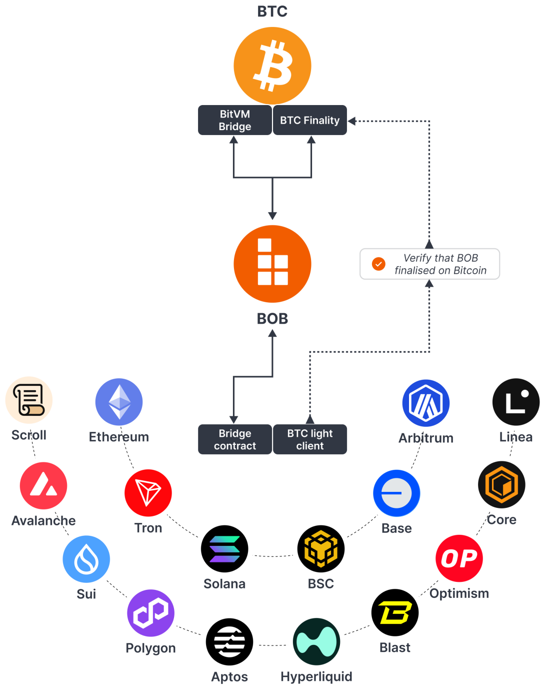

Figure 2: Any L1 chain that can operate a Bitcoin light client, e.g. via a smart contract, can create a trust-minimized bridge to BOB.

operate trust-minimized bridges secured by Bitcoin to any smart contract chain that can verify the Bitcoin blockchain. This means 90% of the modern L1s and L2s, including Solana, Tron, Sui, Aptos, Monad, Avalanche, Cosmos, Polkadot,... the list goes on. Users of these chains will deposit native assets such as ETH, SOL, TRX, DOT into BOB, trade against BTC or other digital assets, and withdraw back to the respective L1 chain - all as long as Bitcoin is secure. Instead of trusting Binance or Coinbase, users trust Bitcoin. Instead of relying on 3rd party bridges, users rely on Bitcoin to secure multi-chain deposits and withdrawals.

Using Bitcoin as a trust-anchor to create an interoperable DeFi ecosystem is the superpower of the Hybrid L2 design. Instead of fragmenting BTC liquidity across dozens of chains, BOB will concentrate liquidity around Bitcoin as trust-minimzed alternative to centralized exchanges, positioning BTC at the center of DeFi.

6 Roadmap

Phase 1: Bootstrapping as an ETH L2 BOB first launched as an Ethereum L2 built with the OP stack[4], operating a native Ethereum bridge, and supporting multiple 3rd party Bitcoin bridges.

Phase 2: Bitcoin "Soft" Finality In Phase 2, BOB will add Bitcoin finality to the Ethereum L2 setup. Once per epoch (one or more BOB blocks), the Sequencer requests a sign-off by participants of the Bitcoin finality protocol[5], who fully validate the BOB chain state. Using BitVM, we can then construct a trust-minimized Bitcoin bridge secured by this Bitcoin "soft" finality protocol, i.e., to attack the Bitcoin bridge one would need to corrupt the majority of Bitcoin finality protocol participants (hash rate or BTC stake). The Ethereum bridge will remain secured by Ethereum. Thereby, Bitcoin "soft" finality can be used to accelerate withdrawals of the Ethereum bridge, reducing the delay from 7 days to a few minutes/hours.

Phase 3: Full Bitcoin Security The final step is inheriting Bitcoin security as described in Section 4.1. In the absence of a Bitcoin fork enabling on-chain zk-verifiers, BOB will have to leverage optimistic verification via BitVM. Achieving optimistic rollups on Bitcoin without additional trust assumptions, requires using the Bitcoin mainchain as data availability layer. The associated costs are onerous and pose a challenge in terms of economics. As a result, to complete the transition to Phase 3, BOB must reach sufficient scale in terms of active users such that incurring additional data availability fees does not increase transaction fees beyond that of competing Ethereum L2s. Alternative data availability layers can be considered as a trade-off between cost and security, as they introduce additional trust assumptions beyond that of Bitcoin.

7 Conclusion

The BOB Hybrid L2 is a new approach to solving Bitcoin's limited expressivity and the resulting lack of DeFi capabilities. By inheriting security from Bitcoin and using this to create trust-minimized bridges to Ethereum and other L1 smart contract chains, BOB changes how BTC is used in DeFi. Instead of wrapping BTC to other networks via centralized bridges, users deposit BTC and other assets into a Bitcoin-secured DeFi environment.

8 Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of BOB Foundation or its affiliates. These are subject to change without being updated herein.

References

[1] Jens Groth. 2016. On the size of pairing-based non-interactive arguments. In *Advances in Cryptology–EUROCRYPT*. Springer, 305–326.

[2] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten. 2018. Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*. 1353–1370.

[3] Robin Linus. 2023. BitVM: Compute Anything on Bitcoin. *URL: https://bitvm.org/bitvm.pdf* (2023).

[4] Robin Linus, Lukas Aumayr, Alexei Zamyatin, Andrea Pelosi, Zeta Avarikioti, and Matteo Maffei. 2024. BitVM2: Bridging Bitcoin to Second Layers. *URL: https://bitvm.org/bitvm_bridge.pdf* (2024).

[5] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J Knottenbelt. 2021. Sok: Communication across distributed ledgers. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25*. Springer, 3–36.

[4] https://docs.optimism.io/

[5] Two Bitcoin finality protocols currently in testing are merged mining and Bitcoin staking. A key factor in this decision is ease of verification in BitVM.