Execution Layers

The next piece of the puzzle in making BTC useful is designing the chain that facilitates this use with the best possible UX. Multiple considerations go into how developers want to design this chain.

- Execution environment – Should it be an Ethereum Virtual Machine (EVM) compatible chain? Being EVM compatible has its advantages, such as,
    - Several years' worth of available tooling, such as wallets and bridges to other EVM chains, is at the disposal of developers.
    - The UX is familiar to users.

  Ethereum's L2s have already benefited from EVM compatibility. L2s like Arbitrum and Optimism that were EVM compatible could quickly gather users and applications already on Ethereum. In contrast, L2s like Starknet that are not EVM compatible struggled to gain adoption.

  However, EVM has its disadvantages, too. Because EVM executes transactions serially, parallel processing is not possible. Newer execution environments, however, like the Solana Virtual Machine (SVM) and the upcoming Monad, allow parallel processing.
- Data availability – Similar to Ethereum, a few rollup solutions are also emerging in the Bitcoin landscape. Depending on how and where they store data, rollups have multiple flavours. Some store state differences (differences in two states of the chain after executing a batch of transactions) on the L1 along with validity proofs, some store compressed transaction data on the L1, and some only store only the validity proof on the L1 with transaction data on a separate layer. Some chains like Stacks use Bitcoin as a checkpointing mechanism. Block time on Stacks is much lower than Bitcoin's. Stacks post data from its blocks between two Bitcoin blocks onto every Bitcoin block.

  Execution layers can post transaction data on Bitcoin in the form of inscriptions. Recall the 6.66 kbps bandwidth of the Bitcoin network. If I take 10 bytes (10 bytes is generous typically; this would be ~20 bytes) as the size of a compressed transaction, a Bitcoin block can include a theoretical maximum of ~600 compressed transactions. However, this maximum is almost impossible since 4 MB blocks are a rare phonemon and it is even rarer that the entire 4 MB space is available for inscriptions. The block size depends on the mix of SegWit and non-SegWit transactions. SegWit, short for Segregated Witness, separated or segregated transaction data from witness data. The idea was that not everything stored in a block is of equal value. Instead of limiting the block size to the traditional 1 MB, SegWit proposed a new limit of 4 million weight units. So if a block had all non-SegWit transactions, the limit would be 1 MB. But if it had all SegWit transactions, it could be a 4 MB block.

Several teams are building layers of Bitcoin to tap into BTC's massive liquidity. For this article, we looked into six different teams that make different trade-offs and have interesting designs. We briefly describe how they work, their development stage, and their traction so far.

Babylon

Babylon focuses on expanding the use of BTC as a staked asset. It brings in a different approach than the rest of the Bitcoin layers (the so-called L2s) in the form of remote-staked BTC. What this means is instead of locking BTC on Bitcoin to mint a synthetic version on a different layer, Babylon introduces the following mechanism –

1. A user locks their BTC in a self-custodial vault by creating a UTXO that can be spent only once, either when the pre-specified time (staking period) has passed or when the user burns their staking UTXO through their special EOTS (extractable one-time signature).
2. After confirming the staking transaction, the user can use their EOTS to validate blocks on PoS chains in the Cosmos ecosystem to earn a yield.
3. If the user behaves honestly, they can unlock their BTC at the end of the staking period or submit an unbonding transaction to Bitcoin.
4. If dishonest behaviour is detected, the user's EOTS is revealed to the public. How is this detected? Babylon's vigilantes ensure at least one honest operator. It is a program suite that acts as a relayer of data between Bitcoin and Babylon. The submitter program submits Babylon checkpoints to Bitcoin using OP_RETURN. The reporter programme scans Babylon checkpoints and reports them back on Babylon. If an anomaly is detected, anyone (called a slasher) can use the public EOTS key and submit a Bitcoin transaction to claim the malicious user's stake. An obvious question is why users can't use the key themselves and get the stake back. The answer probably is that when the miner sees this transaction and if someone else initiates the same transaction, the miner will pick up a transaction with a higher fee. For example, if the stake in question is 5 BTC, the slasher can share even 4.99 BTC with the miner and be profitable. In this case, the miner keeps most of the profit instead of the slasher. However, the malicious user loses most of their stake, either to the slasher or the miner.

Although Babylon provides an interesting approach to expanding the use of BTC, the mechanism is fairly complex. For example, slashing has yet to be successfully implemented on many PoS chains, even though some of the have been live for years. Additionally, although Babylon can utilise remote staking so that BTC can be used to secure other PoS chains, it needs a bridge to enable other BTC use cases like lending.

Build on Bitcoin

Better known as BOB, Build on Bitcoin is ironically an Optimism-based rollup that settles on Ethereum as of June 2024. It claims to be a Bitcoin-aligned Ethereum L2. BOB will launch in four phases –

- Phase 1 – OP stack rollup. It is purely an Ethereum rollup in this phase. Fraud proofs are not yet live on the mainnet. Fraud proofs are a mechanism that allows anyone to challenge the validity of transactions included in a rollup batch.

- Phase 2 – Ethereum rollup with Bitcoin's security. In this phase, BOB will utilise Bitcoin's merged mining. Merged mining allows miners to secure (or mine on) multiple chains along with Bitcoin.
- Phase 3 – Optimistic Bitcoin rollup via BitVM. BitVM is not live currently. As it goes live after improving upon the current version, BOB will start settling on Bitcoin using BitVM.
- Phase 4 – Zk rollup on Bitcoin. After Bitcoin accepts an opcode that allows it to verify Zk proofs, BOB will use Zk proofs to settle on Bitcoin.

As of June 17, 2024, BOB has a TVL of ~$60 million, with Sovryn DEX contributing ~$20 million.

Botanix

The Botanix team brought about a significant innovation: the Spiderchain. What is Spiderchain? It is a rolling multisig of orchestrator nodes on Botanix. Let's break it down. As we mentioned earlier, an L2 needs a bridge and a chain that executes transactions. An orchestrator node keeps users' funds secure on Bitcoin and mints and burns synthetic BTC (on the EVM layer) for users. Orchestrators run Bitcoin and Spiderchain EVM (Botanix) nodes.

Let's say there are N orchestrator nodes on the network. M (<N) orchestrators are randomly chosen for every Bitcoin block to secure incoming BTC. Every epoch, new keys are generated with a new set of orchestrators. While bridging out, the last BTC is chosen first to ensure that older and established orchestrators control older coins.

Botanix's chain is EVM-compatible and secured by a PoS consensus mechanism. Along with securing BTC on Bitcoin by participating in a rolling multisig network and facilitating minting and redeeming synthetic BTC, orchestrators also participate in the EVM chain's block building. They post the root hash, a compact version of the Botanix EVM transactions, as an inscription in Bitcoin. Readers must note that merely posting data on Bitcoin doesn't mean settlement. The difference here is that the data that external chains like Botanix post in the form of an inscription gets stored in a place not validated by Bitcoin nodes (miners). The Bitcoin protocol is entirely unaware of this data. Thus, it cannot be determined whether the transaction data posted in the inscriptions is correct.

As of June 2024, Botanix EVM and Spiderchain are in the testnet phase.

Citrea

Citrea is building a Zk rollup on top of Bitcoin. What does 'on top of Bitcoin' mean? Just that it intends to use Bitcoin as the data availability layer. It says that *the most secure and incentive-aligned way to scale Bitcoin blocks is to shard the execution with on-chain verifiability and data.* Sharding the execution means breaking execution into smaller pieces. Citrea then aggregates shards or batches of transactions and posts the state differences between the two transaction batches on Bitcoin along with a proof known as the validity proof. But the problem is that Bitcoin doesn't have the capability to verify any proofs at the moment. The final form of Citrea will have to wait until Bitcoin has opcodes that allow it to verify zk proofs.

In the meantime, it will use a BitVM implementation as a stop-gap arrangement for proofs and to bridge BTC in and out of the rollup. Naturally, Citrea inherits BitVM's drawbacks mentioned in the previous section. In the future, as BitVM improves, Citrea will improve its bridge functionality.

Citrea is in the testnet phase as of June 2024.

Mezo

Mezo touts itself as the economic layer of Bitcoin. It does not call itself a Bitcoin L2. It uses Threshold Network's tBTC bridge (mentioned above) to bring BTC in and out of the EVM chain, Mezo.

Mezo is being built by the same team that has built products like tBTC, Fold, Keep, and Taho. The team has been building applications around Bitcoin for years. Mezo's aim is simple: to expand the use cases of BTC. It does so via three mechanisms –

1. Letting Mezo users earn a yield by staking BTC to secure the network.
2. Letting users pay gas fees in BTC, which is distributed to veBTC and veMEZO stakers.
3. Building an end-to-end BitcoinFi experience.

What do BitcoinFi and the economic layer even mean? Most new chains, including the EVM ones, rely on existing UX — the same wallets, bridges, etc. Revamping the UX is almost never a priority. Mezo is curating the whole UX from the ground up, something I have rarely seen. It includes;

- A native stablecoin (mUSD) backed by BTC so that users don't have to bridge from other chains.
- A long-tail lending protocol guaranteed by BTC.
- A fully integrated on and off-ramp via Fold.
- An integrated wallet experience via Taho.

Mezo is based on the Cosmos SDK. It uses Comet BFT for consensus.

CometBFT is software for securely and consistently replicating an application on many machines. By securely, we mean that CometBFT works as long as less than 1/3 of machines fail in arbitrary ways. By consistently, we mean that every non-faulty machine sees the same transaction log and computes the same state. Secure and consistent

*replication is a fundamental problem in distributed systems; it plays a critical role in the fault tolerance of a broad range of applications, from currencies to elections to infrastructure orchestration and beyond. (*Source: https://docs.cometbft.com/v0.37/introduction/)

It consists of two components—a consensus engine and a generic application interface. Based on the Tendermint core, the consensus engine is responsible for block production, validation, and finality. Tendermint was one of the first proof-of-stake consensus designs. It offers Byzantine Fault Tolerance (BFT) consensus and can tolerate up to one-third of malicious nodes.

The application interface, Application BlockChain Interface (ABCI), separates the consensus engine from applications. A major advantage of ABCI is that since consensus and applications are separated, developers are not mandated to build applications in the same language in which the consensus engine is built. The interface acts as a medium that delivers transactions to applications for execution. This capability makes the system more modular and helps target more application developers. Initially, Mezo will only be compatible with the EVM runtime.

Mezo's economic design means that, as it gains prominence, BTC holders may benefit directly or indirectly. They can either stake BTC on Mezo and earn staking yield or, if they choose to keep holding their BTC on Bitcoin, they will derive some benefit from BTC being taken out of circulation (to pay for fees on Mezo).

Mezo has a dual-staking model, as shown in the image below. Validators on the network can stake both BTC and MEZO (the native token of Mezo Network). By staking BTC and MEZO, validators get veBTC and veMezo, respectively. The 've' stands for validator escrowed, and these tokens are typically locked in a smart contract. Validator escrowed token holders have governance rights, and network rewards and fee revenue are shared with them. The longer an asset is locked, the more ve-tokens are given out. veBTC stakers earn BTC, and veMEZO stakers earn MEZO rewards. A part of the MEZO reward can be burned to grow the BTC treasury.

Yield is one of Mezo's core offerings because the fees paid by users are paid to validators who stake BTC. Mezo is set to further expand the scope of BTC staking by offering liquid staking with Acre, Mezo's sister project. When a user deposits BTC into Acre, they get a liquid staked token, stBTC, in return. Deposited BTC is used across chains and DeFi applications. Yield generated through these activities accrues in stBTC, which is 1:1 redeemable for BTC.

With over a trillion-dollar market capitalisation, BTC is not even scratching the surface of the lending market. The distribution of WBTC used in the lending markets is shown in the image below. It shows that the amount of WBTC used in the top three lending applications decreased from ~50k to ~23k between July 2023 and June 2024. The decline of total WBTC in lending applications can be attributed to a 48% decline in WBTC supply,

from 285k WBTC in May 2022 to just over 150k WBTC now. This decline is primarily due to the market realising the risk of centralised parties amidst the aftermath of Luna, 3AC, and Alameda.

In its first phase of the launch, Mezo has already started accepting BTC deposits with three lock-up periods: two months, six months, and nine months. Deposits attract points in the form of a HODL score. One BTC generates 1000 points daily, and a multiplier is associated with lock-up periods. A higher lock-up period implies a higher multiplier. Users can also deposit other assets like USDe, USDC, and USDT to get a boost on their BTC deposits. As of July 2024, Mezo's TVL stands at $135 million.

In addition to rewarding holders, Mezo will share a portion of their fees with the Bitcoin core protocol.

Stacks

Stacks, formerly known as Blockstack, recently rolled out its much-awaited Nakamoto upgrade aimed at solving issues like constant forks and slow transactions before the upgrade. Stacks works on proof of transfer (PoX) consensus. So, Bitcoin miners interested in producing blocks on Stacks need to send some BTC. A miner, say, Alice, is chosen randomly to produce blocks on Stacks. The BTC from this miner is given to users who stack (lock/stake) STX, the native token of the Stacks chain. This is interesting because although it's a small yield, it is in BTC. On most chains, the yield is offered only in the chain's native token.

Once chosen, Alice can produce Stacks blocks until the end of the Tenre (next Bitcoin block). As the miner produces Stacks blocks, they are shared with signers for validation. Once more than 70% of the signers accept the Stacks block, it is accepted on the Stacks network. Let's assume that Alice produces 10 Stacks blocks before the next Bitcoin block is mined and that Bob wins the subsequent tenure to produce Stacks blocks.
Bob takes the hash of the first Stacks block that Alice produced on Stacks and adds it to his block commit transaction to the Bitcoin chain. Stackers detect this transaction. They include a tenure change transaction on Stacks that includes the last block's hash, the 10th block in this case, that Alice produced on Stacks. This way, Bob understands that he has to build on Alice's previous block, #10.

Although these are the early days of development for Bitcoin layers, here's a comparison of the above-described chains. It considers chain design, bridge design, and the dollar value secured.

We must mention that in addition to the teams mentioned above, many others, such as Alpen, Bison, BitLayer, Rootstock, SatoshiVM, and Soveryn, have been building extended layers of Bitcoin. Readers can find the list here.

The relationship between L2s and L1

L2s help the L1 with two things – scale and cost. They provide users with an avenue to transact much more cheaply without giving away too much security (or any security in the case of L2s with non-custodial, trustless bridges and no additional security assumptions).

Take Ethereum L2s as an example. As per Token Terminal, in the second week of June 2024, Ethereum supported 7.1 million transactions for $10.6 million in revenue. The cost per transaction for users comes to ~$1.5. At the same time, five L2s—Arbitrum, Base, Blast, Optimism, and Polygon—supported over 70 million transactions for $2.75 million in fees. That is $0.03 per transaction. We can argue about the quality of transactions, including whether they are bots or the transaction value, among other things. However, the fact is that Ethereum couldn't support that many transactions.

However, a drawback of this is that L1s are no longer directly connected to their customers or users. In the traditional world, it is generally the businesses closer to end users that capture a major chunk of value. Amazon is an excellent example. Its enormous distribution allows it to have the upper hand over suppliers and manufacturers.

Dollar Shave Club disrupted the razor industry by selling directly to consumers via a subscription model, eliminating traditional retail channels. This allowed them to price products at a lower point and retain most of the value rather than sharing it with the entire supply chain.

It is usually a bad idea to add another layer between you and your customer. Why are L1s going down this road, then? By adding L2s to the mix, L1s are not losing customers. They are introducing a B2B mix into a business model that was previously strictly B2C. But there can still be a concern— do L2s get to capture most of the value? Do they pass on enough fees to L1?

Luckily, Ethereum has been down this road over the last three years, and we can observe the impact of L2s on Ethereum's value capture. There are two ways to understand whether L2s have been predatory to Ethereum.

1. The first is whether Ethereum lost revenue to L2s. We can inspect this by examining how Ethereum's revenue share has changed in the Ethereum ecosystem's revenue. The following chart considers the revenue of Ethereum and five leading L2s. Ethereum consistently makes up 90%+ of the revenue stream.

2. Another way is to see the market capitalisation or price. Because value capture is almost always reflected in prices, ETH makes up ~95%+ of the total market value of the Ethereum ecosystem, considering its top 10 L2s by market capitalisation.

Ethereum could not have supported so many transactions, yet it still captures 90%+ of the ecosystem's value, suggesting that L2s have been the correct step forward for scaling Ethereum. As long as L2s settle on L1, healthy competition among L2s for the L1 blockspace bodes well for the health of the base layer.

What's next?

Think of the island analogy again. When it comes to real L2s, the two islands must collaboratively build a bridge. But without the Bitcoin islanders' internal consensus, that's impossible. What's happening right now is those who want to be L2 islands to the Bitcoin island are trying to ensure infrastructure as a stop-gap arrangement. So once Bitcoin islanders agree that they need to bridge to other islands for their growth, L2 islands are ready. Until then, what matters is that instead of trying to find more complex ways to bridge and create L2s, the focus needs to be on using what has worked and using infrastructure that has already been battle-tested.

Everyone is aware of how Bitcoin islanders are set in their ways and take island security very seriously. Any changes to the island are thoroughly debated. Anyone who wants to suggest changes to Bitcoin can draft a Bitcoin Improvement Proposal (BIP). After informal debates on various forums, the author takes in the feedback and makes changes to the BIP. A committee of islanders then gives a number to the BIP, which is when it becomes official.

Some islanders understand the importance of cautiously modernising the Bitcoin island. Teams like Botanix, Taproot Wizards, and Thesis are laying the groundwork for adding opcodes to expand Bitcoin's programmability. BIP-420 (also known as OP_CAT) by Ethan Heilman and Armin Sabouri will bring a plethora of exciting possibilities to Bitcoin. CAT stands for concatenate. It is an opcode that was a part of the original Bitcoin opcodes but was redacted by Satoshi due to security concerns that have now been alleviated as the Bitcoin execution environment has evolved over the years.

The opcode allows two pieces of data to be joined together. It unlocks numerous possibilities from custom transaction types like dynamic escrow systems, smart contracts like atomic swaps, different DeFi applications, and greater interoperability with external chains.

Teams like Starkware have already suggested that OP_CAT can bring STARK verification to Bitcoin. This means that Bitcoin can verify Zk proofs, thereby enabling rollups. This design paradigm not only allows general-purpose designs on Bitcoin but also improves its scalability, which it desperately needs.

Other designs by the Taproot Wizards team, like CATVM, are already in the works. This design will use OP_CAT to create trustless bridges. Unlike the current BitVM design, CATVM does not have liquidity requirements. CATVM will enable decentralised trading of ordinals and runes with a UX that is as good as other chains.

Segwit paved the way for Taproot, which was, in turn, critical for ordinals. Ordinals and inscriptions made BRC-20 and runes possible. Recent enthusiasm among Bitcoin developers suggests growing support for achieving social consensus on BIP-420. It also helps that it will be backwards compatible, so the network doesn't need a hard fork to activate it. We are excited for it to go live and witness a new era of genuinely Bitcoin-native programmability.

After a long time, there has been a surging developer interest in Bitcoin. All the independent projects that are building around Bitcoin are like small modern islands around the mighty Bitcoin island. With BIP-420, there will likely be ways to fuse these islands together to make one prosperous and modern island.

With all the changes happening to Bitcoin, I hope that in the future, we will be able to use BTC in different financial applications without knowing too many differences about the layers beneath, just like the seven islands of Bombay fused together to form Mumbai.