EigenLayer & Babylon

Decentralized Trust Marketplace built on existing trust - a new paradigm in the crypto space.

Research Report by

Wayne

zwzwkl@hotmail.com

17 Nov, 2023

Product mechanism

Extra Slashing conditions

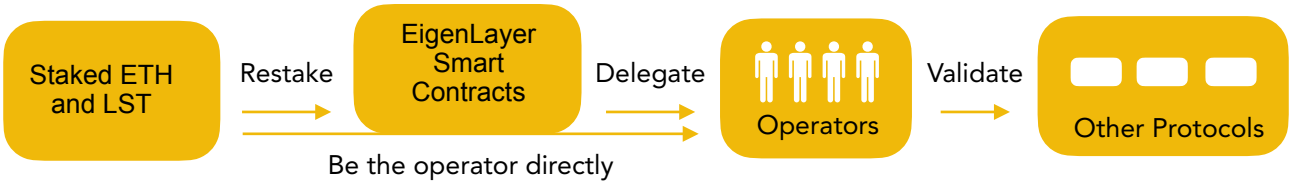
In the blockchain ecosystem, every node has a basic economic incentive: if a node or validator behaves correctly by validating transactions and securing the network, it will receive a reward. However, if a node becomes malicious and attempts to attack the network, it should be subjected to punishment (slashing).

In Ethereum's consensus mechanism, if a validator attempts to sign two blocks at the same height, the validator will be slashed. This means his/her staked ETH will be reduced as a feasible economic penalty.

Therefore, in order to *rehypothec* the trust from Bitcoin and Ethereum to other platforms, it is necessary to implement slashing conditions that incentivize and disincentivize validator behavior. These conditions play a crucial role in maintaining the integrity and security of the network by penalizing malicious actors and ensuring that validators act in the best interests of the system. (Please read ***Appendix 1*** for more background information.)

EigenLayer

EigenLayer has introduced a novel concept called "restaking," which enables validators or users who have already staked their ETH within the network to re-stake their staked ETH (LST) into the EigenLayer protocol. This restaked ETH is then utilized to secure other platforms. By leveraging the restaked ETH, EigenLayer establishes an operator system comprising operators who carry out the actual validation work for other protocols.



This restaking process allows for the reuse of staked ETH. Users who choose to restake their ETH receive additional yield in addition to the rewards they already earn from staking ETH. This is because they are providing validation services for other protocols. However, it's important to note that obtaining the extra yield also comes with additional risk. Users must willingly **opt-in** and be prepared to adhere to the extra slashing conditions associated with the restaking process[1].

EigenLayer protocol builds a marketplace for protocols seeking validation services, known as Actively Validated Services (AVS). Protocols that require such services can now directly rent or purchase them from EigenLayer, allowing them to focus on developing business logic on top of the established trust layer.

EigenLayer emphasizes that bootstrapping the consensus layer and establishing trust is a resource-intensive task. By creating a marketplace for validation services, EigenLayer aims to offer a more efficient and cost-effective solution for protocols seeking to leverage the existing trust and security within the EigenLayer ecosystem.

Governance of extra slashing of EigenLayer

There are two layers of governance in the extra slashing part. The first layer is the on-chain governance, which involves the economic incentives mentioned above. Validators receive rewards or face slashing based on the code written on-chain. It's worth mentioning that different protocols may require different types of Actively Validated Services (AVS) in the trust marketplace. This means that the AVS can be customized, and the slashing conditions can be negotiated and then written on-chain.

The second layer of governance is the social layer. If a situation arises that cannot be addressed by the predefined slashing conditions, there will be an off-chain veto committee to resolve it.

Babylon

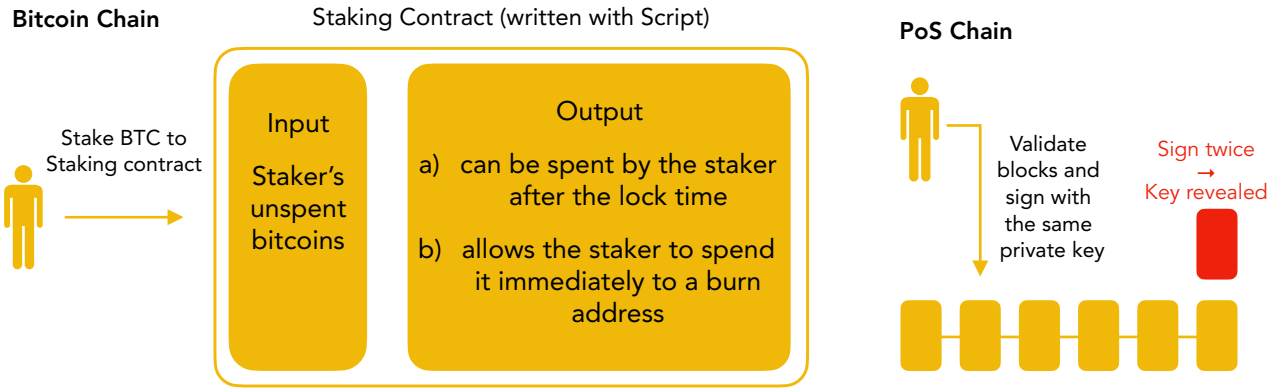
For EigenLayer, as it is built on top of Ethereum, implementing extra slashing conditions is easy with the help of smart contracts. However, Babylon faces a different situation as Bitcoin does not support smart contracts.

What does Babylon want to achieve?

1. Malicious validator will be slashed using Bitcoin's non-Turing Complete programming language
2. Ensuring the safety of staked bitcoins: a) all bitcoins remain in the Bitcoin chain without the need for bridges; b) individuals who stake bitcoins retain control of their private keys (no custody).

How to achieve the goals?

Although Bitcoin does not have smart contracts, its programming language still allows for expressing specific conditions for spending BTC within the UTXO. For example, the staking period (lock time) can be expressed using the OP_CHECKSEQUENCEVERIFY opcode[2], as stated in the Babylon whitepaper[3].



Therefore, if holders want to stake their bitcoins, they can send a transaction with the input being their bitcoins and the output having two possible cases as shown in the graph above. In either case, holders retain control of their bitcoins by holding their private keys.

If the staker behaves properly, the bitcoins will be unstaked after the lock-in period. However, if the staker acts maliciously and attempts to sign two blocks at the same height, their private key will be exposed to the public, allowing anyone to spend the unspent bitcoins in the staking contracts.

Babylon utilizes extractable one-time signatures (EOTS) to achieve this. The idea is that you can sign a message once, similar to normal signature schemes. EOTS requires an additional tag parameter, which, in this case, is the block height. If you try to sign the same message twice with the same tag (signing two blocks at the same height), your private key can be extracted from the two signatures[4].

Babylon chain

Once the biggest challenge is solved, Babylon is able to build a Bitcoin Staking protocol with Babylon chain itself works as the middle layer between Bitcoin and other protocols. As the communication channel, Babylon chain will pass the other chains data (block hashes and signing info) to Bitcoin chain. Once the data is written in Bitcoin blockchain, the security is guaranteed. The communication is actually the process of synchronization using the *Bitcoin timestamping*[5].

Shared security

By leveraging the mechanisms described above, EigenLayer and Babylon tap into the well-established trust frameworks of Ethereum and Bitcoin.

This empowers them to extend their services to other protocols, fostering a decentralized trust marketplace. Instead of undertaking the cumbersome task of building their own node systems and bootstrapping the consensus layer, protocols in need of trust services can seamlessly access a unified trust pool. This approach eliminates the fragmentation of PoS trust pools and ensures the high level of security (as high as Ethereum or Bitcoin).

Risks

The protocol design of both projects have various risks, with one notable concern being the potential strain on the consensus mechanisms of Ethereum[6] and Bitcoin, or the '*social consensus pressure*.' If a

significant amount of value is protected by the shared trust layer, and an issue arises that is considered more critical than Ethereum's consensus, such as a real-world political matter, a social fork could be implemented. Despite Ethereum being fundamentally sound, it might undergo a fork. The concept of trust sharing poses both a potential threat to the original chains and a challenge to decentralization.

Value Proposition to Users

For both EigenLayer and Babylon, they require three types of participants:

- Restakers/Stakers: Users who are willing to restake ETH or stake BTC as a source of security.
- Operators/Validators: Chain operators who provide additional validation services for new protocols.
- Developers/protocols: The "customers" who require staking security services, such as new PoS chains, bridges, and data availability solutions.

The first two are essential for EigenLayer and Babylon to provide services to their target customers. Leveraging the existing trust and security within EigenLayer and Babylon helps eliminate the need to bootstrap the consensus layer, reducing costs. Additionally, in theory, the BTC staked in the Babylon protocol could be *restaked* in EigenLayer.

	EigenLayer	Babylon
Mainnet	Stage 1 launched	Not yet
(Re)Staking Asset	ETH / LST	BTC
Additional Yield	Yes	Yes
Trust Marketplace	Yes	Yes
Low Cost of Bootstrapping Security	Yes	Yes
Target Users	PoS chain, DA services, MEV, Sequencer Layer, Settlement Layer.	PoS chains

The final issue is determining how strong the target users' willingness to pay for the services is.

For EigenLayer, the advantage lies in its alignment with Ethereum. Ethereum has the largest ecosystem in the crypto space, which translates to more users and greater demands. EigenLayer's solution has the potential to address the limitations of Ethereum, such as the need for secure and decentralized bridges, data availability solutions, and a decentralized sequencer layer for Layer 2 solutions. Using ETH as the staking asset is considered "politically correct" within the Ethereum ecosystem.

Regarding Babylon, as stated on its website, the targets are new PoS chains and existing PoS chains seeking increased security. While there are numerous PoS chains, it cannot be expected that more than 100 PoS chains will emerge every year, and not all of them will utilize the services. However, there could be over 1000 protocols within the entire ecosystem, with the majority being ETH/EVM-related. **In a modular blockchain world, the number of chains will be significantly less than the number of modular protocols addressing specific problems.**

Another challenge faced by both protocols is that applying the trust layer eliminates the need to stake protocols' native tokens. On the positive side, protocols are not vulnerable due to the low value of their tokens. If the native token is used, a low value makes it cheaper and easier to attach the consensus. This can overcome the "death spiral" where a token's price decline makes the system more vulnerable.

However, staking is a powerful way to create use cases for tokens and lock up liquidity, reducing selling pressure and improving price performance. Additionally, as a new chain grows larger and stronger, trusting a third party may no longer be the best option. EigenLayer did come up with a dual staking[7] idea where ETH and native tokens both accepted as staked asset. But it is just an idea yet.

In summary, EigenLayer targets a larger and more diverse user base. In addition to chains, the mentioned services have the potential to be adopted by many entities. Ethereum alignment is another crucial factor driving adoption. There are already some early projects building on EigenLayer[8].

Competitive Advantage

	EigenLayer	Babylon
Founder	Academic Background, Uni of Washington	Academic Background, Uni of Stanford
What does the protocol do?	Builds a decentralized trust marketplace on Ethereum	Brings Bitcoin's security to other PoS chains
Ecosystem mainly focusing	ETH	Cosmos
Total Funding Amount	• Pre seed round, unknown amount (May 2022) • Seed round, $14.5M (Aug 2022) • Series A, $50M (Feb 2023)	• Seed round, $8.8M (Jan 2022)
Latest Valuation	$250M (Post A)	N/A
Strengths	• Ethereum alignment and a bigger ecosystem • First and the top protocol in terms of restaking • Launched & LST capacity is already full • More resource brought by the crypto investors	• Huge amount of idle bitcoins • Modular design • Overcomes the additional slashing condition issue without smart contracts
Weeknesses	• Too expensive • Uncertainty in the social governance (veto committee)	• Mostly theoretical • Convinces people to trust and stake bitcoins
Opportunities	• ETH eco (DA, sequencer, L2, bridges, new chains)	• Cosmos eco, app chains
Threats	• Overloads Ethereum consensus and makes Ethereum centralized — Ethereum doesn't like this and need more solo stakers	• Works in theory but infeasible in practice • Be seen as a *DDOS* to Bitcoin like ordinals

If we are being optimistic, restaking or shared security could be a significant narrative in the crypto space. These two protocols are the pioneers in this field. However, if other competitors enter the game, will they be surpassed by new players? Well, probably not.

Security is a highly sensitive sector in crypto. One strategy that new players can employ is to provide higher yields with token incentives, similar to the **vampire attack**[9] conducted by SushiSwap against Uniswap. However, the safety of funds is usually more important than higher yields. Additionally, in crypto history, the first protocol of its kind typically maintains its top position: Uniswap, AAVE, GMX, and Lido.

Team Info

The founder of EigenLayer, Sreeram Kannan and the founder of Babylon David Tse are friends and they have been working together in the crypto consensus mechanism field. They are the co-authors of multiple research papers[10] [11]. The idea of Babylon of reusing Bitcoin's security[12] [13] is also published by them together, along with another co-founder of Babylon Fisher Yu.

EigenLayer Core Members

Most of the core members are from the University of Washington Blockchain Labs, especially engineers. They have been working on consensus mechanisms and how to reuse existing trust for years. Calvin Liu worked as the strategy lead at Compound (a DeFi lending protocol), which was one of the projects that started the DeFi Summer. Divergence Ventures is also a crypto-focused investment fund.

Sreeram Kannan

- Founder & CEO, LinkedIn
- Associate Professor at the Department of Electrical & Computer Engineering at the Uni of Washington
- Studied P2P wireless communication in PhD and moved to Biosystems. Started to do research on blockchain about 5 years ago.
- Head of Uni of Washington Blockchain Lab

Robert Raynor

- Engineer LinkedIn
- Student of Sreeram Kannan

Soubhik Deb

- Head of protocol Research LinkedIn
- Student of Sreeram Kannan

Vyas Krishnan

- Product LinkedIn
- Graduated from UIUC and perviously worked for a global payment company Nium as the product owner.

Calvin Liu

- CSO LinkedIn
- Strategy Lead at Compound for nearly 4 years and he also works for Divergence Ventures

Bowen Xue

- Engineer Link
- Student of Sreeram Kannan

Babylon Core Members

The core members of Babylon are mixed with strong academic backgrounds and crypto native experiences. Apart from the two co-founders, others are form crypto protocols in DeFi, and public chains.

David Tse

- Co-Founder, LinkedIn
- Professor of Engineering at Stanford University
- Member of the U.S. National Academy of Engineering
- Received the 2017 Claude E. Shannon Award from the Information Theory Society

Fisher Yu

- Co-Founder, CTO LinkedIn
- Previously managing Director of Hash Lab, providing crypto security service

Shalini Wood

- CMO LinkedIn
- CMO of e-Money, a DeFi project built on Cosmos from 2021 to 2023 Feb.

Sankha Banerjee

- Head of Product Strategy LinkedIn
- Core member of Nibiru Chain, a DeFi hub on Cosmos from Sep 2022 - Mar 2023
- CEO of Credence Capital, a crypto venture firm from 2019 - Aug 2022

Xinshu Dong

- Technology Strategy X (Twitter)
- Previously the Co-Founder of RockX, Staking solution provider
- Previously the Co-Founder and CEO of Zilliqa, a public chain

Final Thoughts

EigenLayer and Babylon are both decent projects. EigenLayer is building a decentralized trust marketplace on Ethereum by leveraging the existing trust within the Ethereum ecosystem. Babylon aims to unlock idle bitcoins on the Bitcoin chain and develop a staking protocol to serve as a trust layer for new protocols. There are many similarities between these two protocols.

However, from an investment perspective, I personally lean towards investing in EigenLayer rather than Babylon. The specific reasons for this preference include:

- EigenLayer has a better market fit and there are already more than 120k $ETH ($244M) restaked[14].
- The overloading Ethereum's consensus and centralized risks exist but can be mitigated by a close conversation with Ethereum foundation (it is already on-going) and scaling control by the team.
- Babylon in theory can solve the additional slashing condition and non-custody of bitcoins issues, while we don't know in practice the willingness of Bitcoin holders to stake their bitcoins and how the code works.
- Based on the speeches and panel discussions[15] [16] [17] [18] [19] [20] [21] I watched about the two team, EigenLayer's team, especially the founder has a better communication with the community.
- It is a fact that there are already many protocols are been built on top of EigenLayer. Ethereum ecosystem has the biggest communities and users. Politically correct of being Ethereum alignment is also a quite important reason.
- Bitcoin is a reserve asset. Although there are scaling solution / L2, and BRC20 projects in the Bitcoin ecosystem, touching holders' bitcoins is still not the best idea.
- Babylon's success also relies on the development of Cosmos ecosystem to start the first step.
- EigenLayer's TVL would need to increase fourfold to achieve the same ratio (TVL/FDV) as Lido. (Appendix 3)

Appendix 1 Background

The core value of a blockchain is the TRUST it created by its consensus mechanism

Bitcoin was created as a Peer-to-Peer cash system, and its biggest accomplishment was solving the double-spending problem. Proof of Work (PoW) is used as the consensus mechanism to establish a global consensus regarding the order of transactions. Everyone holds the same ledger, and it is completely open and decentralized.

The elegant design of the consensus mechanism establishes the fundamental trust of Bitcoin. It is a system that enables users/nodes from all over the world, who are complete strangers, to collaborate as intended. Tokens serve as economic incentives to ensure the smooth operation of this system.

Before The Merge[22], Ethereum was similar to Bitcoin in terms of the consensus mechanism. It transitioned to Proof of Stake (PoS) after the Paris Upgrade. Instead of relying on nodes' hash power to produce new blocks, it now depends on the amount of ETH being staked.

After years of development, it is now nearly impossible to attack or fork Bitcoin and Ethereum. A Substantial amount of "real money" has been invested in these two systems to secure them and validate transactions. In the case of Bitcoin, this involves the computational power brought by mining hardware. For Ethereum, it involves more than 28 million $ETH (over $56 billion USD) being staked.

Re-use the TRUST

Now that trust has been established, how can it be utilized? Bitcoin primarily focuses on one simple purpose: transferring bitcoins, limited by the non-Turing complete Script language. However, Ethereum offers much more. With the invention of the Solidity programming language, developers can write smart contracts and build various applications on top of the Ethereum network. Nonetheless, Ethereum faces limitations, such as the low transaction-per-second (TPS) problem. The trust layer has limited block space available for developers.

To address these challenges, we have witnessed the emergence of numerous alternative chains and Layer 2 solutions aimed at scaling Ethereum or Bitcoin. Besides developing their own ecosystems, are there other ways to fully leverage the existing trust?

One such project is EigenLayer, a protocol seeking to create a decentralized trust marketplace on Ethereum. It enables the reuse of ETH already staked in the network for new crypto networks through a process called ***restaking***. Another project is Babylon, a Bitcoin staking protocol that allows Bitcoin holders to stake their coins in a trust-less manner while keeping them on Bitcoin chain.

Appendix 2 List of Layer 2s (TVL > $1M)

#	Name	Tech	TVL	MKT Share
1	Arbitrum One	Optimistic Rollup	$7.25B	54.25%
2	OP	Optimistic Rollup	$3.51B	26.25%
3	Base	Optimistic Rollup	$571M	4.27%
4	zkSync Era	ZK Rollup	$434M	3.25%
5	dYdX	ZK Rollup	$420M	3.14%
6	Mantle	Optimium	$158M	1.19%
7	Immutable X	Validium	$148M	1.11%
8	Linea	ZK Rollup	$140M	1.05%
9	Starknet	ZK Rollup	$136M	1.02%
10	Polygon zkEVM	ZK Rollup	$104M	0.78%
11	Loopring	ZK Rollup	$103M	0.78%
12	Metis Andromeda	Optimium	$79.45M	0.59%
13	zkSync Lite	ZK Rollup	$73.40M	0.55%
14	ApeX	Validium	$45.21M	0.34%
15	Scroll	ZK Rollup	$38.18M	0.29%
16	Manta Pacific	Optimistic Rollup	$25.90M	0.19%
17	ZKSpace	ZK Rollup	$25.00M	0.19%
18	Arbitrum Nova	Optimium	$24.97M	0.19%
19	Sorare	Validium	$19.37M	0.14%
20	rhino.fi	Validium	$14.68M	0.11%
21	Aevo	Optimistic Rollup	$10.41M	0.08%
22	Boba Network	Optimistic Rollup	$10.17M	0.08%
23	Zora	Optimistic Rollup	$8.06M	0.06%
24	Paradex	ZK Rollup	$3.20M	0.02%

Source: https://l2beat.com, Nov 17, 2023

Appendix 3 Valuations of EigenLayer

	TVL ($M)	FDV ($M)	MC ($M)	TVL / FDV	TVL / MC
EigenLayer	244	250	NA	0.9760	NA
EigenLayer MIN	244	29.61	26.36	8.2410	9.2550
EigenLayer MAX	244	160.75	58.38	1.5179	4.1792
EigenLayer TVL*5					
EigenLayer MIN	1220	148.04	131.82	8.2410	9.2550
EigenLayer MAX	1220	803.74	291.92	1.5179	4.1792
If we want EigenLayer to have the same TVL/FDV ratio as Lido, what is the TVL needed?					
EigenLayer	2060	250		8.2410	
Statics of other liquid staking protocols					
Lido	17677	2145	1910	8.2410	9.2550
StakeWise	192	75.17	24.24	2.5542	7.9208
Rocket Pool	2286	582	547	3.9278	4.1792
Stader	170	112	21	1.5179	8.0952

Source: Defillama, CoinMarketCap, 17 Nov, 2023

* EigenLayer's TVL is currently capped (LST), with further discussions underway to add more.
* EigenLayer's TVL would need to increase fourfold to achieve the same ratio (TVL/FDV) as Lido.

References

[1] https://docs.eigenlayer.xyz/overview/readme/whitepaper
[2] https://en.bitcoin.it/wiki/Script
[3] https://docs.babylonchain.io/assets/files/btc_staking_litepaper-32bfea0c243773f0bfac63e148387aef.pdf
[4] https://cubist.dev/blog/cubist-babylon-partner-on-anti-slashing-for-bitcoin-stakers
[5] https://medium.com/@wisdomedem88/bitcoin-timestamping-a-different-approach-with-babylon-chain-5f514f7da24a
[6] https://vitalik.ca/general/2023/05/21/dont_overload.html
[7] https://www.blog.eigenlayer.xyz/dual-staking/
[8] https://www.blog.eigenlayer.xyz/twelve-early-projects-building-on-eigenlayer/
[9] https://coinmarketcap.com/academy/article/what-are-vampire-attacks-in-crypto
[10] https://arxiv.org/abs/2005.09610
[11] https://arxiv.org/abs/1910.02218
[12] https://arxiv.org/abs/2201.07946
[13] https://arxiv.org/abs/2201.07946
[14] https://defillama.com/chain/Ethereum?tvl=true
[15] https://www.youtube.com/watch?v=aP9f_1v9Ulc
[16] https://www.youtube.com/watch?v=HcEGXoC57Rw
[17] https://www.youtube.com/watch?v=ywJNXIUSqOw
[18] https://www.youtube.com/watch?v=RG7A0flGJNM
[19] https://www.youtube.com/watch?v=-V-fG4J1N_M
[20] https://www.youtube.com/watch?v=J9IKmZWEn1E&list=PLmxcKDuCA1V5_Le2GMNCDZ5-ELJViZslP&index=12
[21] https://www.youtube.com/watch?v=GSgKBqiktM0
[22] https://ethereum.org/en/history/#paris