⚔️

Scaling and Bridging with Sidechains

Bitcoin approximately does 7 transactions per second. How can it compete with Visa's thousands?

Transactions per second its a metric that perfectly express the idea of that a blockchain can only do a specific quantity of work in a given amount of time.

Bitcoin protocol has ossified a lot, this means that make new changes are extremely difficult, providing a certain robustness to the network. For this reason, the only way to scale a blockchain network is to spawn new chains. These new chains provide further blockspace for their users, lowering network fees across the board. They are run by their own full nodes and block producers/validators.

Communication between chains

It's when users of one chain are able to trade assets securely with users of another. Communication takes place entirely at the level of *bridges* between two chains. Bridges are an essential piece of blockchain networks: their design and properties almost entirely determine the security of the network as a whole.

Bridge Model

Lets consider two chains: Origin and Destination. Both run the same protocol and EVM-based chains, but they are operated by separate sets of full nodes. The state of Origin is obtained by executing all transactions published in Origin's chain of blocks, and the same goes for Destination.

Alice notices that Bob, a Destination user, owns the latest Catatat, a limited edition NFT minted on Destination. Bob has put the NFT for sale, priced at 50 UND, a stablecoin produced by the United Nations. Alice happens to have 100 UND in her Origin account. She wants to bridge 100 UND to Destination to facilite the purchase of the Catatat. Alice must find a bridge to Destination.

Essentially, a bridge is an account on Origin, which takes custody of assets received from users of Origin. Once the bridge receives the assets, some mechanism creates an equivalent balance on the Destination chain, crediting the user with their assets on the other side. This model is known as a two-way pegged bridge.

Sidechains: Scaling out with parallel chains

With increasing congestion and increasing transaction fees on "Layer 1" networks, sidechains were introduced to release the pressure. A sidechain is simply a new blockchain, running in parallel to the "parent chain", with a bridge between the two to move assets around. On Ethereum, popular sidechains include Binance Smart Chain (BSC) or the Polygon PoS chain.

How sidechains work?

- It involves a parent blockchain (like Ethereum) called Origin, and a sidechain called Destination.
- Block producers on Destination reach consensus on the current state of all user account balances on Destination.
- This agreed state is summarized into a short "commit" string by hashing all the account values together.
- The commit is published on the Origin chain, serving as a compact commitment to Destination's current state.
- Using cryptography, a user like Bob can prove to Origin that his 50 UND balance on Destination is consistent with the published commit.
- When Bob wants to withdraw his 50 UND from Destination to Origin:

    1. He proves to Origin that he owns 50 UND on Destination, using the commit.
    2. He proves to Origin that he initiated a withdrawal from Destination.

- The withdrawal proof (like a proof-of-burn) is important to prevent double-spending of the "virtual" UND minted for Bob on Destination.
- It ensures the virtual Destination tokens removed from Bob's balance match the tokens locked in Origin's bridge contract.

In essence, the commit is a compact representation allowing Origin to verify user balances and state transitions on Destination without storing Destination's full data. The cryptographic proofs enable secure asset transfers between the chains.

Security of a sidechain

The main threat to the security of sidechains is corruption of the state by the set of block producers, e.g., "printing money" on the sidechain and withdrawing it all to the parent chain. The level of decentralization among block producers is critical to gauge the security of the sidechain.

Scaling Tradeoffs

- Sidechains boost scaling parameters like decreasing block times or increasing block sizes
- This results in a smaller set of more resourced block producers and validators
- Reduced decentralization among this smaller validator set is a security risk

Main Security Threat

- The primary threat is block producer collusion to corrupt the sidechain state
- E.g. "printing money" by crediting accounts illegitimately and withdrawing to parent chain

Attack Example

- Alice deposits 100 UND from Origin's bridge contract to get 100 UND on sidechain Destination
- She sends 50 UND to Bob, who withdraws correctly to Origin

- Colluding Destination validators credit 50 UND to Carol illegitimately
- Carol is able to withdraw these 50 UND from Origin's bridge, draining it
- Alice is now unable to withdraw her remaining 50 UND

Implications

- The bridge's security is reliant on the security of the connected chains
- A centralized sidechain can put user funds at risk of theft by validators
- Even without theft, censorship of withdrawals by validators can "freeze" user funds

Sidechains sacrifice some decentralization for scaling, making them inherently more insecure, especially when connecting lower and higher value chains. Careful management of validator sets and decentralization is crucial for maintaining security guarantees.

Bridge hacks!

There are two more ways in which the bank analogy holds. The first has to do with robberies, and the second with bank runs.

 Nothing nets them a higher reward than stealing from the source directly, bank vaults. Bridge contracts are similar in this respect. As users deposit more assets to be bridged, the bridge contract holds greater and greater amounts, sometimes billions of dollars. This makes bridges a very attractive target to exploit.

At least 5 validators out of 9 registered on the bridge must sign a transaction vouching for the deposit or the withdrawal. A “multi-signature" (multising) bridge design is quite popular, and doesn't require a separate consensus from a decentralized set of validators. The validators registered in the multisig contract are usually well-known entities, or partners to the sidechain project.

The "bank run" may take place as a consequence of a hack. Users of the sidechain, seeing that their assets on the sidechain are no longer backed by an equivalent basket of assets held by the bridge, precipitate to withdraw before the bridge is emptied. The same phenomenon is sometimes observed when doubts are cast over an exchange's solvency, or with asset-backed stablecoins.

Conclusion

The security of a scaling solution is equal to the security of its weakest link. Thinking about sidechains already allowed us to discuss two specific threats, that will reappear throughout:

1. How is the user protected against theft of their assets?
2. Can the user assets be frozen?