# Core Chain: Unlocking Bitcoin DeFi

The Core blockchain (Core Chain) is the first Bitcoin-aligned EVM blockchain, designed to be Bitcoin's complementary and hyper-scalable smart contract platform. The mainnet launch of Core Chain introduced Satoshi Plus consensus, a combination of Delegated Proof of Work and Delegated Proof of Stake that incorporates Bitcoin miners and mining pools in the security of a scalable smart contract platform. In the coming months, a third leg is being added to Satoshi Plus consensus in the form of non-custodial Bitcoin staking, allowing any bitcoin holder to earn yield by staking their bitcoin tokens without giving up custody.[1]

Additionally, Core Chain is gaining trustless atomic swaps between itself, Bitcoin, and EVM chains more generally, along with Core-native wrapped bitcoin (coreBTC) and other Bitcoin-related infrastructure improvements. This will facilitate the growth of a Bitcoin DeFi (BTCFi) ecosystem, of which Bitcoin is the primary benefactor and beneficiary. **The dimensions of this ecosystem shouldn't be underestimated; there is nearly $1T worth of bitcoin waiting to be unlocked via BTCFi (at today's prices), and the size of the market for Bitcoin-based smart contracts alone could be north of $230B.**[2]

In essence, a blockchain can be described as a network of aligned incentives stewarding the security of a system or systems. Various blockchains are tailored for distinct purposes; some focus on processing thousands of transactions per second, others secure extensive databases, and many facilitate smart contracts, adding layers of complexity to their operations.

The Bitcoin blockchain is a network of incentive-aligned stakeholders stewarding the security of the bitcoin asset. In the course of performing their day-to-day activities, Bitcoin miners, nodes, users, etc. uphold the essential properties which have made bitcoin akin to digital gold – its hardness (finite supply), decentralization, immutability, transparency, censorship-resistance, and permissionlessness.

---

[1] Following standard usage, the word "Bitcoin" with a capital "B" refers to the overall network, and "bitcoin" with a lowercase "b" refers to the digital asset.

[2] These numbers were pulled from https://bitcoinlayersreport.com/ on February 13th, 2024 (the report must be downloaded).

Due to Bitcoin's importance as a perfectly sound, gold-like store of value, the network is designed with purposeful limitations at the protocol level to maximize its preservation and permanence over its scalability. These intrinsic limitations impact Bitcoin's speed, complexity, composability, interoperability, and flexibility. To take just one example, Bitcoin does not natively support Turing complete smart contracts like those that constitute DeFi ecosystems on EVM-compatible blockchains. Nevertheless, Bitcoin's simplicity, while sometimes cited as a weakness, is really the core strength of the protocol.

A valuable case study relating to proposed evolutions of the bitcoin protocol is the debate over expanding Bitcoin's block size, known as the Blocksize War. While intended to scale Bitcoin as a viable payments network, expanding Bitcoin's block size could lead to centralization as fewer participants would be able to afford the storage, bandwidth and processing power required to run a full node. Therefore, Bitcoin's existing block size can be understood as a component of the incentives that guide decentralized stakeholders in securing the bitcoin asset.

While the capacity for peer-to-peer transactability is essential, Bitcoin's role is not to serve all global payment needs, but rather to defend bitcoin as a decentralized store of value.[3] Non-core functionalities are peripheral. Any scaling solutions that fail to contribute to aligning the incentives that preserve bitcoin's essential properties are, at best, neutral.

Despite Bitcoin's block size remaining the same, proponents of greater block size nonetheless forked the protocol into Bitcoin Cash. While Bitcoin Cash succeeds in terms of speed and cost, it fails in terms of decentralized consensus, incentive-alignment, and continuity. Ultimately, by competing for security budget resources, Bitcoin Cash became a parasite threatening, albeit impotently, to dilute the value of both itself and Bitcoin. The cornerstones of what makes bitcoin valuable were cast aside for the sake of a functionality that the network was not designed to optimize in the first place. Bitcoin Cash was an attempt to fit a square peg in a round hole.

What lessons should be drawn from this? **Increasing Bitcoin's utility and performance requires solutions that do not change the base layer.** Bitcoin layer 2 solutions like sidechains, channels, and statechains are designed to accomplish scalability by building directly on top of Bitcoin. The Lightning Network, for example, is a layer 2 designed to support faster and more

[3] In the case of larger block size, even a hundredfold increase wouldn't suffice for it to function as a large-scale payments network.

cost-effective transactions. While it did succeed in delivering quicker and cheaper transactions, the presence of operational complexities, liquidity issues, and other technical barriers have kept it from being the breakthrough for mass-adoption that many envisioned.

As this example illustrates, building directly on top of Bitcoin means inheriting many of its limitations. The result is often a lack of sophistication in terms of use-cases and a surplus of complexity in terms of the user and developer experiences.

Given Lightning's struggle to build a global payments platform on Bitcoin, the prospect of Bitcoin being a scalable base layer for virtual machines, smart contracts, and other such complexities is even more daunting. Nevertheless, projects like Stacks and Rootstock have introduced smart contracts on top of Bitcoin. These approaches do open the door to increased utility, but ultimately face similarly inherited limitations.

In designing an optimal Bitcoin-secured smart contract platform, the key inheritance is not the Bitcoin base layer's rigid technical infrastructure. Rather, the crucial inheritance is the network of incentive-aligned stakeholders. Together, these facts imply that the key to unlocking Bitcoin DeFi lies in **expanding Bitcoin incentive-alignment beyond the mere bitcoin asset and onto a smart contract platform**.

Core Chain is that smart contract platform. It aligns the interests of both chains' stakeholders by introducing a parallel and symbiotic consensus model, Satoshi Plus. Together, Nakamoto Consensus and Satoshi Plus Consensus reinforce one another, simultaneously defending the bitcoin asset and Bitcoin-powered smart contracts, respectively.

## How Does Core Chain Work?

Core Chain was designed with many goals in mind, including:

- Leveraging Bitcoin to secure a decentralized, permissionless, trustless, censorship-resistant, self-sovereign, Turing Complete, and multi-purpose blockchain.
- Expanding Bitcoin governance, incentive-alignment, and protection to EVM-compatible smart contracts.

- Unlocking Bitcoin DeFi by granting Bitcoin stakeholders easy access to a parallel Bitcoin-secured, Bitcoin-aligned, and hyper-scalable smart contract platform.
- Providing Bitcoin miners with increasingly-needed supplemental rewards by having them recycle hash power through Delegated Proof of Work.
- Using mechanisms like non-custodial staking to turn bitcoin from a passive asset into a productive one (*without* entering new blockspace), thereby enabling far more bitcoin use-cases while reinforcing its core functionality.

The center of these ambitions lies in Core Chain's novel Satoshi Plus consensus mechanism, the two basic components of which are a pioneering Delegated Proof of Work technique that leverages the hash power of Bitcoin miners, and Delegated Proof of Stake, which is well known throughout the blockchain world. In the next few sections, these topics will be covered in more detail.

## Delegated Proof of Work

The Bitcoin network is the most decentralized and secure in the world, thanks in large part to the work of Bitcoin miners and the incentives that guide them in turning physical energy into digital gold. With Core Chain, those incentives are now extended to power a multi-purpose smart contract platform. This requires no additional costs or complications to the miners' most important job of defending the bitcoin asset. On the contrary, miners earn additional supplemental rewards, which further incentivizes Bitcoin mining.

To participate in securing Core Chain, miners simply write two additional pieces of information in the `op_return` field as they produce a new Bitcoin block:

1. The address of the Core Validator the miner wants to delegate their hash power to.
2. The address that the miner would like its CORE token rewards to be sent to.

In exchange for participating in the consensus process by delegating their hash power to vote for Core Validators, miners receive supplemental CORE token rewards in addition to their existing bitcoin rewards. Core Chain is therefore entirely symbiotic with Bitcoin. Satoshi Plus receives Bitcoin miner participation and Bitcoin receives better compensated (i.e. more highly incentivized) miners.

### Delegated Proof of Stake

Satoshi Plus was based in part on a recognition of the fact that the users of Core Chain must be involved in the consensus process alongside Bitcoin stakeholders. Delegated Proof of Stake is the method of achieving this balance. To participate in consensus, any CORE token holder can stake their CORE tokens with Core Validators, thus voting for those Validators in the same way that a miner might delegate its hash power to vote for them.

Similarly, just as miners receive rewards, CORE token stakers also receive CORE token rewards for contributing to Satoshi Plus consensus. One particular advantage of Delegated Proof of Stake compared to standard Proof of Stake models is that the former permits all token holders to participate equally, while the latter sometimes only permit large holders to stake.

## What Sets Core Chain Apart?

Having covered the basic operations of Core Chain and how it offers unique advantages in building a Bitcoin-based DeFi ecosystem, the next topic is a discussion of how Core Chain is different from protocols designed with similar ambitions.

### Stacks

Stacks is a Bitcoin layer 2 seeking to bring some of the ideas from the broader DeFi ecosystem to Bitcoin. Though this goal is laudable, Stacks' lack of EVM-compatibility is a critical drawback. Ethereum developers wanting to build on Stacks have to learn an entirely new language to do so – a language that's neither Turing complete nor portable to other ecosystems. These same developers face no such hurdle when building on Core Chain.

Additionally, Stacks' block times are presently long and unpredictable; transactions-per-second on the Stacks chain leave much to be desired, which further deters its use. Improvements are certainly coming to block production and throughput with their Nakamoto update, but even after that goes into effect, Core Chain will have advantages in both areas.

## Rootstock

Rootstock is an EVM-equivalent chain that aims to be a smart contract platform supporting Bitcoin DeFi through the creation of decentralized applications and similar use cases for which the Bitcoin layer 1 is poorly suited. But so far, Rootstock has been relatively unable to attract a meaningful base of developers and users. Moreover, because Rootstock is EVM-equivalent and not EVM-compatible, there's a substantial increase in the burden placed on developers wanting to build on top of it.

Some of the comments made above about Stacks also apply to Rootstock, inasmuch as Core Chain's blocktimes are ten times faster, and its transactions-per-second are multiples of Roostock's theoretical amount.

## Botanix

Through its Spiderchain primitive, Botanix hopes to bring the benefits of the Ethereum Virtual Machine to Bitcoin. But, as with Rootstock, Botanix is EVM-equivalent rather than EVM-compatible, meaning developers face additional challenges in building with it.

More broadly, Botanix is highly experimental and unproven. It operates under a variety of new trust assumptions, with perhaps the most important being that their chain relies on a multi-signature (multisig) structure. As the Liquid project demonstrates, this is a challenge to widespread adoption.

Finally, a lack of field testing makes it difficult to know for certain whether these assumptions will stand up to real challenges. It remains to be seen if Botanix's theoretical block times and transaction-per-second will match the standard set by Core Chain.

## Sovereign Rollups

Pioneered by providers such as Chainway and Rollkit, Sovereign Rollups (SRs) enhance transaction throughput and smart contract capabilities by processing transactions off-chain using independent consensus mechanisms. These systems then anchor a summary or proof of those transactions onto the Bitcoin blockchain by leveraging its data availability.

In their current state, there are no fraud proofs for these off-chain executions, and the single sequencer models that underpin SRs rely on trust assumptions that could potentially undermine the decentralization prized by crypto enthusiasts. It's unclear if these "MEV" opportunities will be exploited in the wild post launch.

Finally, they rely upon the introduction of new op_codes into the Bitcoin protocol, and there are no assurances that such codes will be forthcoming. Historically, making any alteration to Bitcoin has proven extremely difficult, and that may very well be the case with these proposed updates.

### Babylon

Babylon is a Bitcoin restaking protocol that allows its users to stake idle bitcoin without bridging or relying on trusted intermediaries, offering altcoin yields in exchange. Babylon will enable part of what Core Chain was meant to achieve (i.e. through non-custodial bitcoin staking), however, its goal is not to create a DeFi ecosystem backed by Bitcoin.

Moreover, Core Chain's Satoshi Plus consensus could accommodate restaking. And, in future updates, Core Chain may support bitcoin stakers and Bitcoin miners playing a role in its governance, which would further differentiate the two offerings.

## How Does Core Chain Make Bitcoin DeFi Possible?

Despite its prominent stature, bitcoin has hitherto existed as an untapped, passive asset. Expanding its utility and interoperability has proven elusive, but recent advances with respect to staking, wrapping, and swapping are opening up these frontiers at long last.

The next few sections discuss the implementations of these techniques on Core Chain, how they work, and why they're important.

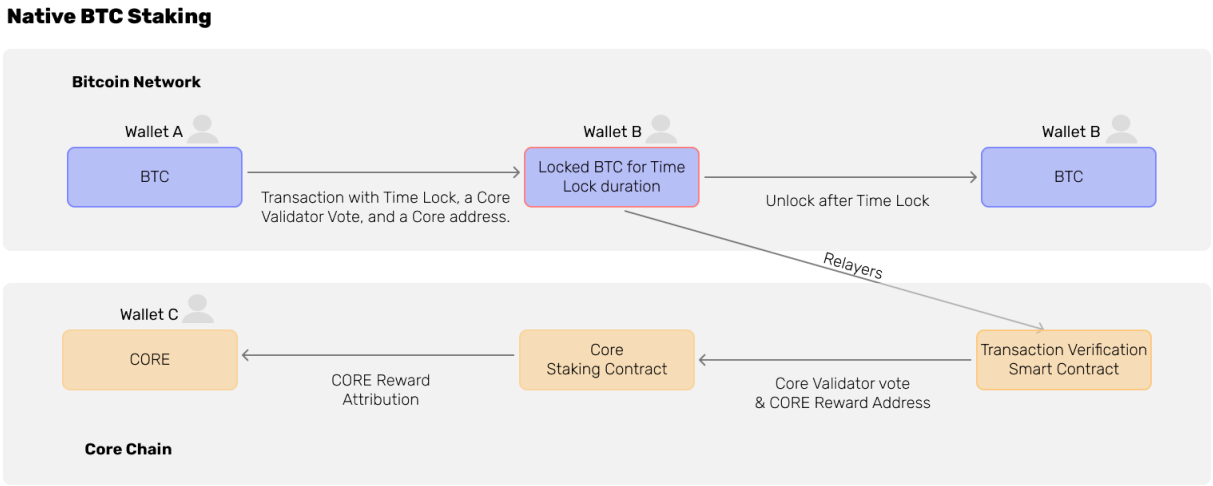
### Non-Custodial Bitcoin Staking

With the introduction of non-custodial bitcoin staking, Core Chain's recent protocol updates incorporate bitcoin holders as the third part of Satoshi Plus consensus.

Core Chain's methodology for integrating bitcoin staking centers on absolute time locks, a Bitcoin-native cryptographic feature that locks up the outputs of a transaction for a pre-defined period of time, during which they can't be spent. Rather than holders giving up custody of bitcoin to external staking, stakers on Core Chain merely need to place their bitcoin in absolute time locks as part of a transaction, and the transaction can be designed to return the output after the time period has elapsed. Within that transaction, stakers must include a script containing the same information that Bitcoin miners include in their delegated blocks[4]:

1. The address of the Core Validator the staker wants to delegate their bitcoin to.
2. The address that the staker would like their CORE token rewards to be sent to.

Bitcoin stakers earn a yield on their otherwise passive bitcoin in the form of CORE token rewards, for however long they set the time-lock (and thus for however long they delegate their bitcoin to vote for Validators on Core Chain). The end result is that billions of dollars in underutilized Bitcoin value will become productive, remunerating stakers while also expanding the scope of Bitcoin's utility.




Core Chain's native bitcoin staking offers a number of benefits.

1. It is designed specifically for the kind of long-term holders and institutions who have shown a clear preference for keeping their assets on the Bitcoin blockchain. Recognizing

[4] See the section above on Delegated Proof of Work for additional clarity.

that such entities are accustomed to holding their bitcoin without frequent transactions, native bitcoin staking offers them the opportunity to earn rewards during a specified holding period.
2. No new trust assumptions are added. Users can stake their bitcoin without moving it off the Bitcoin blockchain, thereby maintaining the high security and trust that comes with Bitcoin's robust infrastructure.
3. It furnishes an opportunity for bitcoin holders to earn passive CORE token rewards in exchange for contributing to Core Chain's consensus.

Furthermore, there are a few aspects of Core Chain's implementation of staking that set it apart.

1. There is no need to transfer your assets. Unlike other DeFi protocols that require transferring bitcoin to a different blockchain or wrapping it, Core Chain's staking allows users to stake directly within the Bitcoin ecosystem.
2. Core Chain's bitcoin staking maintains the basic blockchain ethos by allowing bitcoin holders to contribute to the expansion of Core Chain's overall security budget.
3. There are options to stake through the command line or a web interface, and there's a simple claim process for rewards. The product is designed for ease of use, catering to both tech-savvy users and those preferring a more straightforward approach.
4. The reward system helps align cross-chain incentives. The reward pool comes from a shared consensus reward system that integrates the contributions of both Bitcoin miners and CORE token stakers, thereby optimizing the reward distribution for all participants. Additionally, the rewards are sustainable over the long-term, and will be distributed over a period of 81 years.

## Core-Native Bitcoin Wrapping (coreBTC)

The most common method for bridging assets from a source chain to the target chain is by wrapping assets, which locks them on the source chain and mints a synthetic representation of them on the target chain. When Bitcoin is the source chain, the synthetic asset is wrapped bitcoin. Redemption of wrapped bitcoin for bitcoin involves the holder burning the wrapped asset to trigger the unlocking of their original bitcoin. As long as the wrapped bitcoin is backed 1:1 with bitcoin and users have the ability to redeem, wrapped bitcoin maintains a value equivalent to bitcoin's.

Wrapped bitcoin has gained widespread acceptance in various DeFi environments, particularly with EVM-compatible blockchains. However, prior implementations have encountered significant centralization issues, as the process of minting and redeeming wrapped bitcoin tokens is predominantly controlled by a singular centralized entity. This structure fundamentally undermines trustlessness, resulting in a security profile markedly inferior to bitcoin.

Given Bitcoin's unique value proposition as the most secure and self-sovereign store of value, the bar for a bitcoin-pegged asset is immensely high. Any wrapped asset meant to fully unlock bitcoin's supply must necessarily inherit certain foundational principles, including security, decentralization, trustlessness, permissionlessness, and censorship-resistance. These are the highest priorities for Core Chain's native wrapped bitcoin asset, coreBTC.

The nodes responsible for securely holding users' bitcoin on the Bitcoin blockchain are called Lockers. Anyone can register as a Locker on Core Chain by locking up collateral, and the Core DAO itself will be running one of the many Lockers on offer.

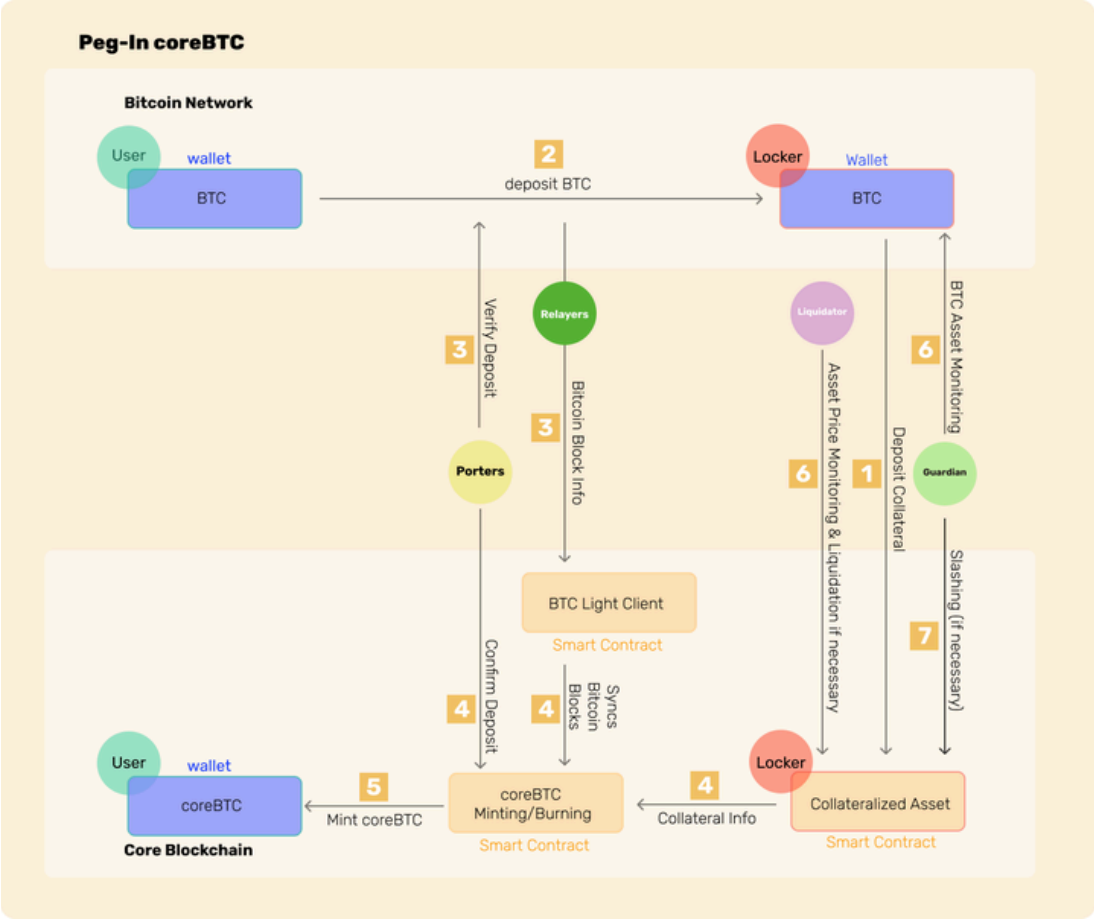
The particular assets and required collateral ratio are network parameters determined by the Core DAO, and the collateral deposited by Lockers means that locked bitcoin should always be backed by assets of a higher value. If there's a change in the price of bitcoin relative to the value of the collateral, the Locker must adjust its collateral or face potential liquidation.

Additionally, collateral serves as a deterrent against malicious behavior, and can be slashed if Lockers transfer bitcoin without authorization or do not promptly return bitcoin when coreBTC is burned. Lockers can unregister and retrieve their collateral at any time, as long as they have no residual bitcoin locked and have no unfulfilled unlocking requests. In exchange for the services provided, Lockers earn small fees.

For minting coreBTC, a user identifies legitimate Lockers and sends bitcoin to a Locker's Bitcoin address. This action is intended to lock their bitcoin as a request and precursor to obtaining an equivalent amount of coreBTC. A Porter monitors the Bitcoin blockchain for incoming transactions to the Locker's address and detects the user's request for coreBTC; after a sufficient number of confirmations on the Bitcoin network, the Porter submits it to a smart

contract on Core Chain with proof of the bitcoin transaction. Porters eliminate the need for users to engage with both Bitcoin and Core Chain separately, a time-consuming process that would involve transaction fees on each chain.

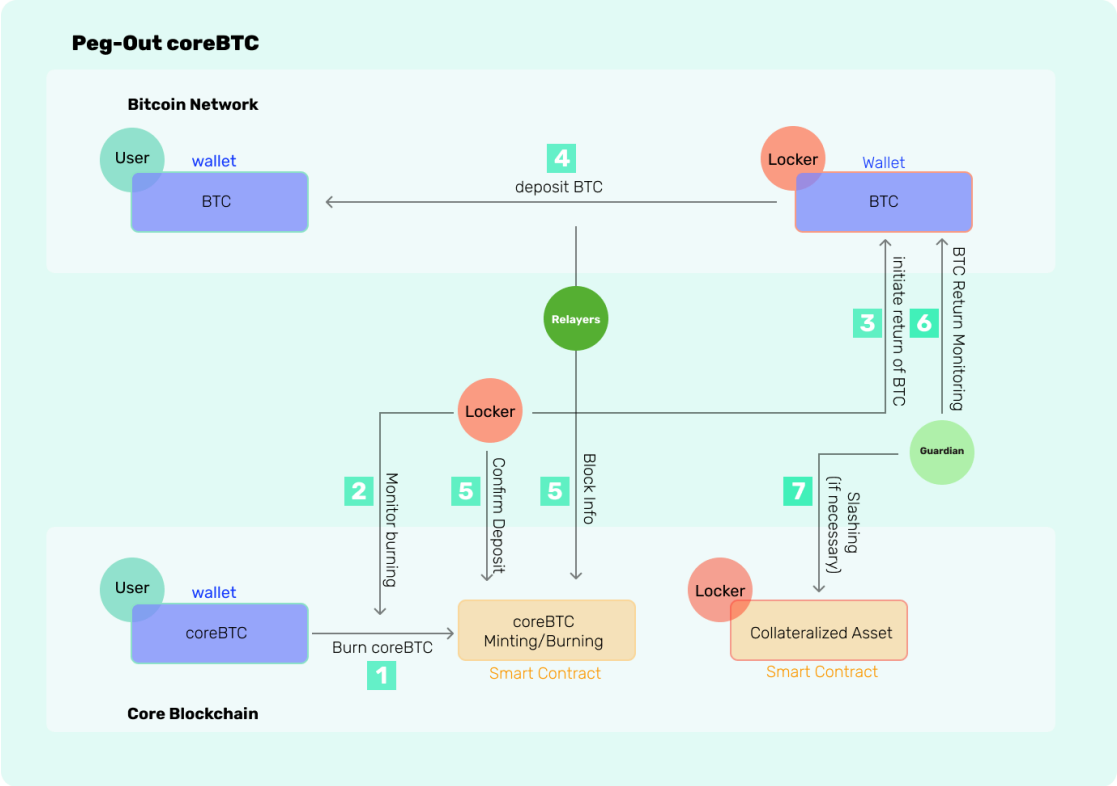
Upon receiving the request, the coreBTC smart contract calls the bitcoin Light Client to verify the authenticity and finality of the relevant bitcoin transaction, and an equivalent amount of coreBTC is then minted.




To redeem coreBTC for bitcoin, a user sends a request to a Core Chain smart contract to burn a specified amount of coreBTC which contains a Bitcoin address where the user wishes to receive their bitcoin.

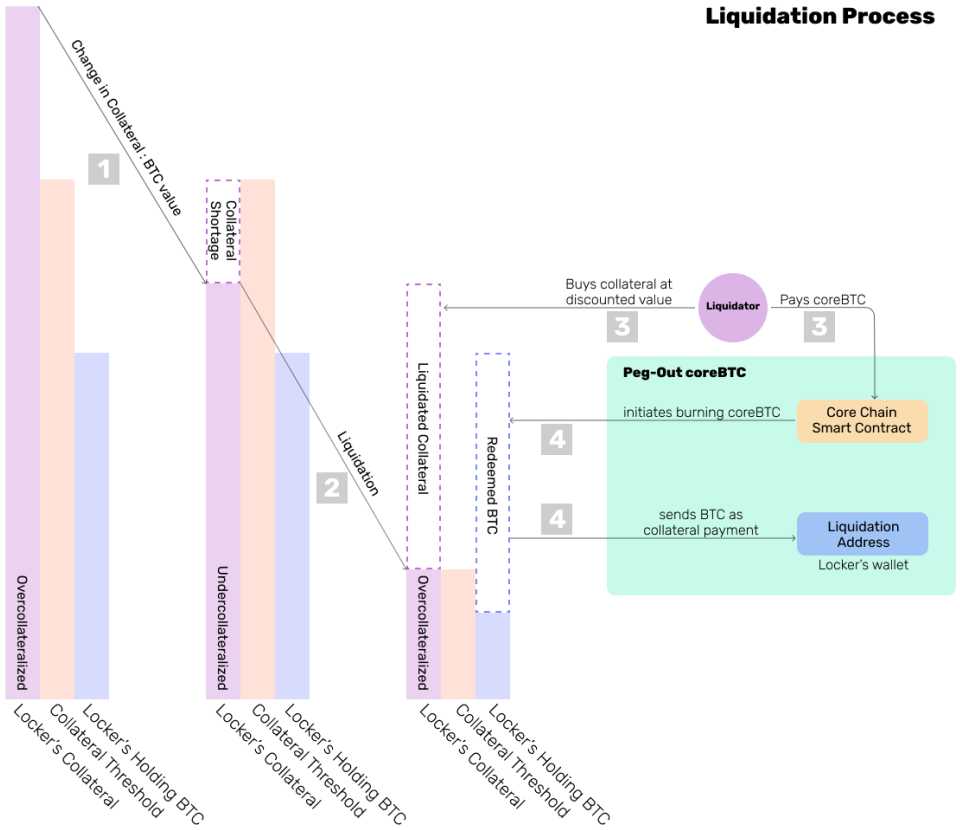
The smart contract then burns the specified amount of coreBTC, removing it from circulation on Core Chain. Afterward, the smart contract alerts the Locker to release the equivalent amount

of bitcoin to the user's address. Upon receiving the alert, the Locker unlocks the bitcoin and sends it to the right address. Once the bitcoin transaction is confirmed, the Locker transmits it to Core Chain where it is finally verified by the bitcoin Light Client.




Throughout the minting, redeeming, and intermediary periods, entities called Liquidators are watching over the health conditions (i.e. collateral ratios) of all Lockers. As the value of the collateral begins to drop relative to the value of the bitcoin locked, Liquidators begin to force liquidation of the collateral. During the process, the Liquidators use coreBTC to buy the collateralized CORE tokens at a discounted price, and the coreBTC is burned. This pushes the

collateral ratio up and restores the Locker to a healthy condition.

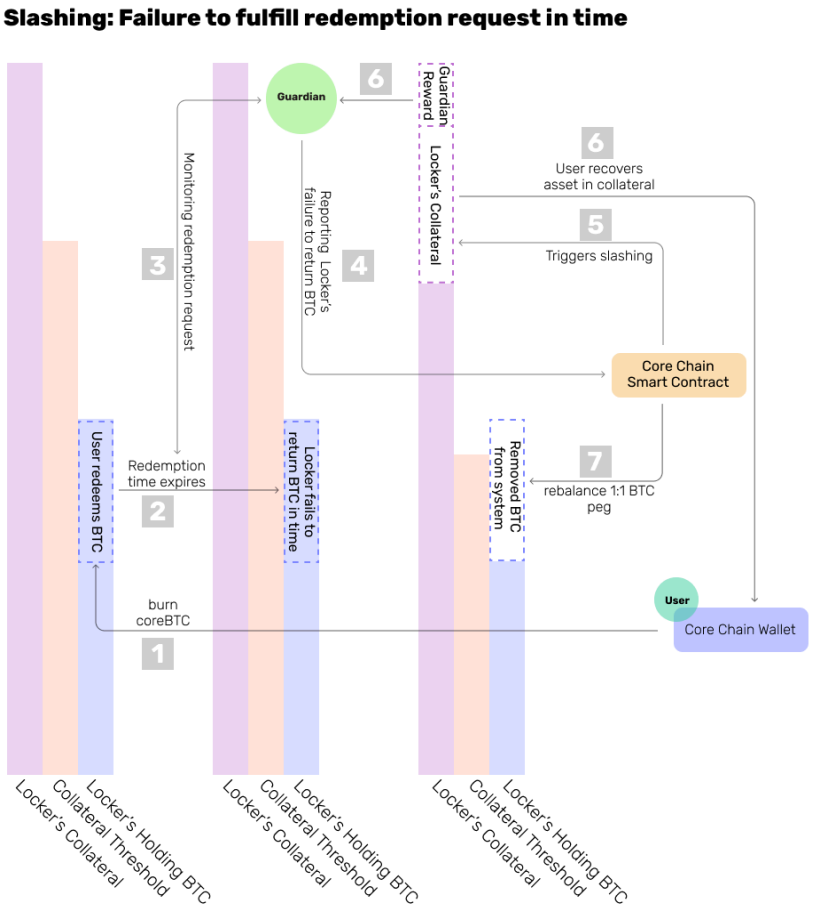



When the coreBTC is burned its supply is reduced and it becomes more scarce, thereby freeing the Locker to take ownership of a quantity of the underlying bitcoin *equivalent to the value of* the eliminated coreBTC. The Locker is then rebalanced in accordance with the collateral requirements; if the original user who sent bitcoin to that Locker's address wants their bitcoin back, they can choose any Locker to get it from. Redemption of coreBTC for bitcoin occurs at a *systemic* level, it's not a relationship between one user and one Locker.

In addition to liquidation, slashing is another critical component in maintaining the value of coreBTC. Since every coreBTC is backed by an equivalent value of locked bitcoin, Lockers must (1) never move locked bitcoin without being prompted by a burn request, and (2) must always promptly redeem locked bitcoin to users who submit burn requests. Failure to perform either of these functions results in the Locker's deposited collateral being slashed. The activity of Lockers

is monitored by Guardians, who check for any misbehavior and apply slashing as appropriate. Users can act as slashers, but Core Chain has implemented Guardians to stand eternal vigil against Locker malfeasance. Users can also become Guardians permissionlessly.

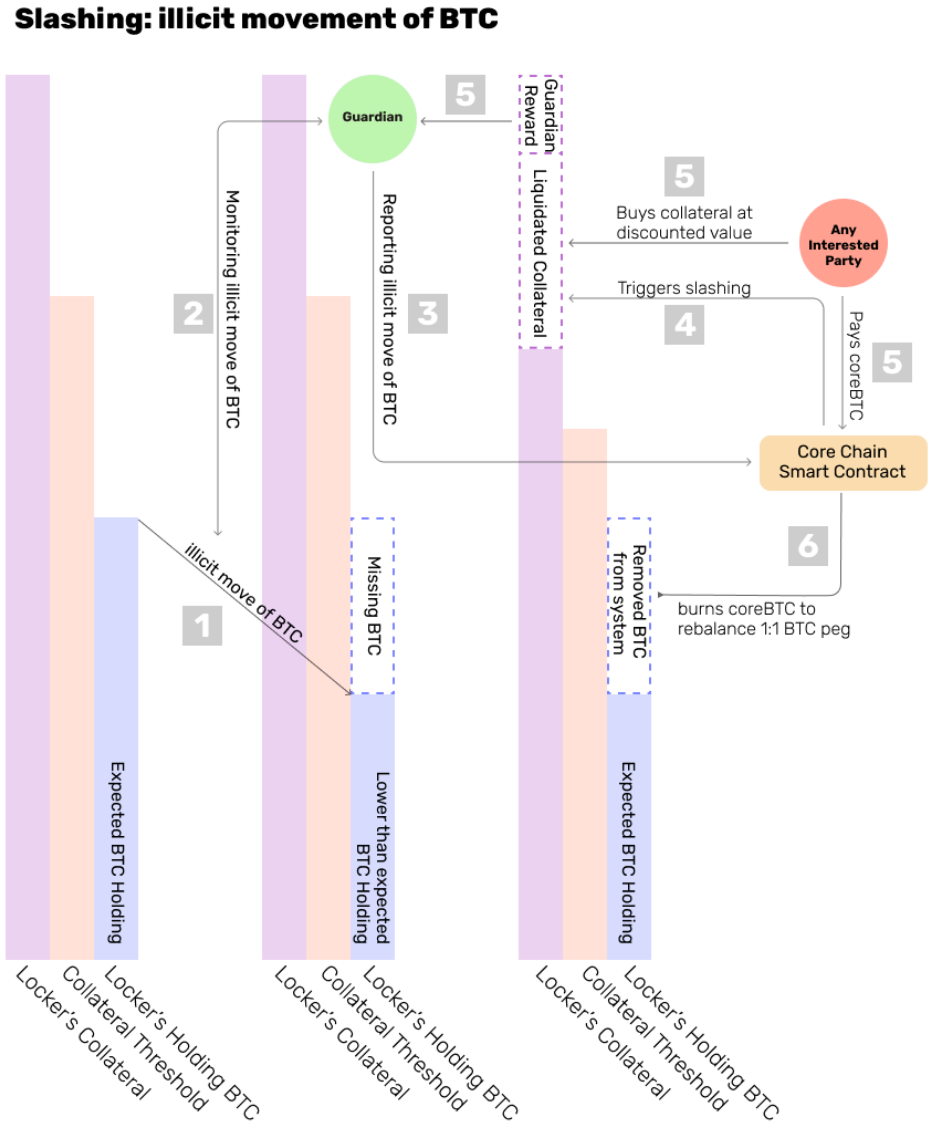
If a Locker doesn't fulfill a redemption request within the specified deadline, a Guardian can trigger Core Chain smart contract to slash some of the Locker's collateral. In this event, a portion of the Locker's collateral, equivalent to the value of the user's burned coreBTC, is transferred to the user. Additionally, the slasher is rewarded with a percentage of this collateral value for their action.




If a Locker illicitly transfers locked bitcoin, a slasher can notify Core Chain smart contract about the violation by presenting details of the unauthorized transaction. Core Chain smart contract then confirms that this transaction doesn't align with any legitimate burn requests and,

once the amount of stolen bitcoin is established, a segment of the Locker's collateral is sold at a discount for coreBTC. The process of selling off slashed collateral is designed to accumulate an amount of coreBTC equivalent to the misappropriated bitcoin *in addition to costing the Locker more value than they stole*, thereby disincentivizing malicious behavior.

The collected coreBTC is subsequently burned by Core Chain smart contract, ensuring that each coreBTC is backed by an equivalent amount of bitcoin. Additionally, the slasher is rewarded with a percentage of the malicious Locker's collateral.



## HTLC Atomic Bitcoin Swaps

HTLC Atomic Swaps enable trustless, peer-to-peer exchange of tokens between Core Chain and other blockchains, including (and especially) Bitcoin. Hashed TimeLock Contracts (HTLCs) combine cryptographic hash functions with timelock mechanisms to ensure that:

1) Either both parties gain access to the other's funds, or
2) Neither party does.

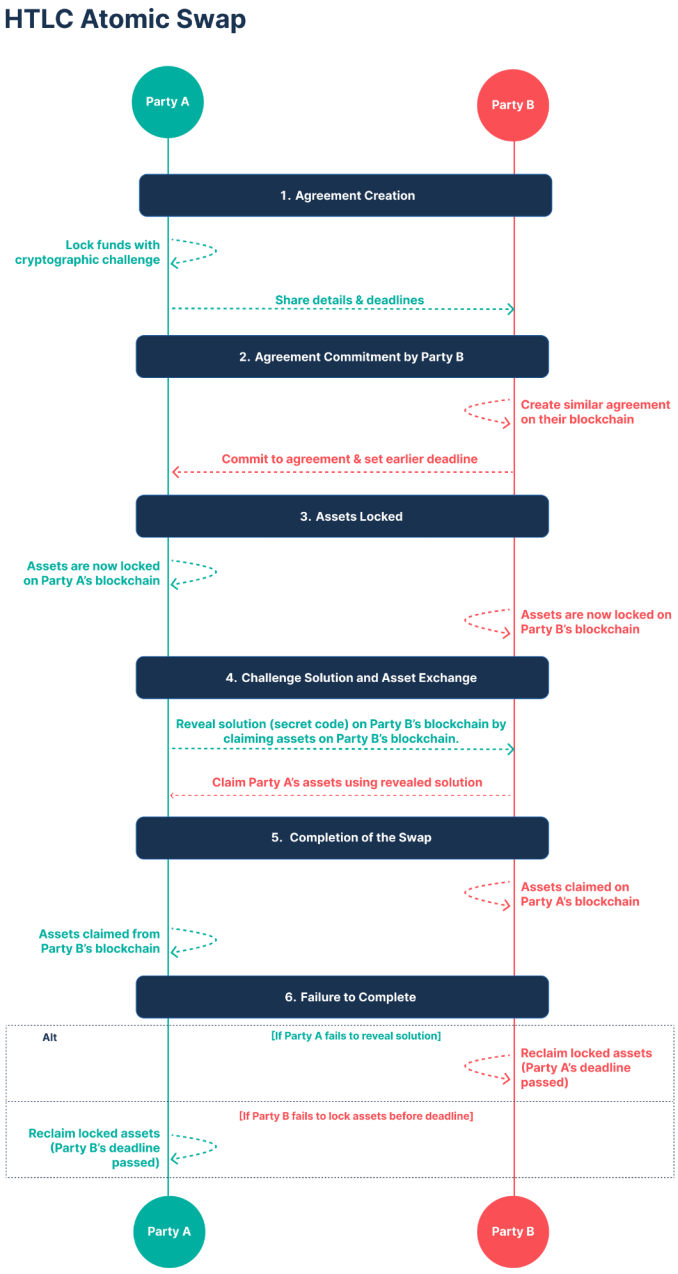
HTLC is a cryptographic technique which confers the ability to lock transactions with a hash function and set additional time constraints on when the tokens can be spent.

Given its simplicity, HTLCs are the most Bitcoin-friendly and secure way for cross-chain value transfer. They enable fully trustless swaps of native assets between Bitcoin or EVM blockchains, and Core Chain, without the need for a centralized authority, oracle, or relayer. Atomic swaps between these networks can also involve other assets, like ERC20, BRC20, NFTs, Ordinals, and more. This introduces a new method of interoperability and makes it simpler to access liquidity between Bitcoin and Core Chain.

As for the atomic swapping *process*, it is initiated when Party A creates a binding agreement by locking their assets within an HTLC on their blockchain. The trustlessness of this contract is underpinned by a cryptographic challenge, consisting of the hash of a uniquely generated secret key, known only to Party A at the outset. The contract further stipulates a precise deadline for the transaction's completion. Party A's commitment then becomes part of the blockchain where it's viewable by Party B, and Party B responds by locking up *their* assets on *their* respective blockchain, utilizing the same HTLC mechanism as Party A. Party B also sets a deadline for this transaction that comes *before* Party A's deadline; for cryptographic reasons that are beyond the scope of this paper, this mitigates the possibility of a time-based refund attack.

At this juncture, the assets of both parties are securely locked within their respective HTLCs, effectively isolating them and making them inaccessible to any external entities. Assets in an HTLC remain locked until the relevant cryptographic secret is used to unlock them. When Party A reveals the solution to the cryptographic challenge (the secret code) on Party B's blockchain, Party A is able to claim Party B's locked assets. Since this revelation makes the solution publicly

accessible on the blockchain, Party B can then utilize the now-known secret to unlock and retrieve Party A's locked assets, thereby completing the exchange. [5]




[5] This does not mean that *anyone* with the secret can unlock the HTLC, because the signer of the unlocking address must be the *other* party to the transaction. HTLC scripts are set up such that unlocked funds are automatically sent to the correct wallet, so even if someone else invokes the transaction, the funds will go to the appropriate address.

The atomic swap ensures that the transaction is either completed in its entirety, or not at all. In scenarios where Party A fails to disclose the secret prior to Party B's deadline, the latter retains the ability to withdraw their assets. Conversely, should Party B neglect to claim Party A's assets after the secret is revealed and before the expiration of Party A's deadline, Party A is granted the right to withdraw *their* locked assets.

As with Bitcoin, the fundamental strengths of HTLC atomic swaps lie in their simplicity and security, but these attributes can also be seen as constraints. The rigidity of these agreements requires both parties to actively and concurrently engage in executing their part of the transaction. Though this simultaneity ensures security, it also lacks the flexibility of placing orders on an orderbook or settling immediately (unless everyone is online at the same time). To address these limitations, a new implementation of atomic swaps has been devised that incorporates a novel market-making protocol. This will enable market-makers to fulfill orders and makes instantaneous transaction settlement possible.

This proposed system would offer a familiar order-book UX to users wanting to execute an HTLC-based atomic swap. The fundamental operation of this system hinges on its ability to continuously provide match-making across disparate blockchain networks. Upon the identification of congruent orders – i.e. orders that correspond in terms of asset type and quantity on both chains – the system would automatically initiate the HTLC process between the matching parties. This procedure guarantees that the assets are securely swapped between them.

The elegance of this system lies in its potential to be invoked by any participant in a completely trustless manner, thereby democratizing access and participation. Users are not required to actively seek and negotiate with counterparties; instead, the system autonomously identifies and pairs matching orders, significantly streamlining the transaction process. This approach not only expands the utility of HTLCs but also enhances their efficiency and the user experience, aligning that experience more closely with traditional financial market mechanisms while maintaining the decentralization and trustlessness for which the Bitcoin blockchain is famous. There’s also an incentive to provide liquidity as a market-maker, as market-makers can add transaction fees in exchange for settling swaps.

## Future Directions

Core Chain is a constantly-evolving ecosystem that maintains an eye on the future, and this section will cover a number of major projects in that vein.

First, Core Chain's governance might expand over time to include both bitcoin stakers and bitcoin miners. This is important because it could increase the alignment between Bitcoin and Core Chain, and also make it easier to bridge assets from the Bitcoin network to Core Chain. Today, there are many bitcoin holders who are not comfortable with this process, meaning that they're less likely to engage actively in BTCFi. Core Chain's expansion of its governance structure to include miners and bitcoin stakers may help ameliorate this issue. In addition, though bitcoin stakers are rewarded in CORE tokens today, in future updates they could be rewarded directly in bitcoin.

Second, Core Chain may take on local fee markets that make bitcoin transactions faster and predictably cheaper. Recall that the original vision for bitcoin was to have it act as *money*, which isn't possible unless it supports fast, cheap, predictable, scalable transactions. The hope is that local fee markets will bring these properties to bitcoin for the first time. The Solana project has gone part of the way towards validating this idea.

Third, there may be a few additions to the way HTLC atomic swaps work that could make them more general purpose. Liquidity pools could be added to supplement the order books that currently underpin the swap process, which would make fills of partial orders possible while reducing the need for market makers.

Fourth, there may also be a strengthening of the trustless nature of coreBTC through the integration of Core Chain's consensus mechanism with multisig wallets. Lockers could also be given more options for collateral, which might expand the pool of potential Lockers operating on Core Chain.

Fifth, in future iterations, staking may be modified such that holders could participate in decentralized finance (DeFi) without the need for wrapping. This would allow those users to preserve their assets in their native form.

Finally, Core Chain is capable of supporting Bitcoin as a means of payment, and this may be fleshed out more fully at a later date. If those changes go live it will mean a person could use bitcoin from start to finish on Core Chain after swapping bitcoin for coreBTC.