

Whitepaper



BTH NETWORK

BTH TOKEN

Decentralized Bitcoin Sidechain
powered by Bitcoin miners and an
innovative new Blockchain.

Bitcoin Layer 2



BitHarvest

A Decentralized Bitcoin Sidechain
Powered by a New Blockchain

Last Updated: Dec 27, 2023

Version 1.2

Abstract

This whitepaper introduces the BitHarvest Network, a new blockchain and token as the incentivemechanism for truly decentralized internet and infrastructure.

The BitHarvest Network and protocol solves various challenges the bitcoin miner faces today. Bitcoin is a Proof-of-Work chain but it is also a \$700 Billion asset and most of it is idle capital and the built-in halving mechanism in Bitcoin's code leads the minting of new Bitcoins will stop once the cap is reached. By the year 2140, miners will stop receiving block rewards and will solely depend on transaction fees.

First, we propose the concept of Proof-of-Calculation (PoC) which allows Bitcoin miners to run BitHarvest network nodes, a sidechain of Bitcoin while to not need to sacrifice the existing hash. Second, Bitcoin miners enable an important new use case for Bitcoin and takes a significant step towards integrating Bitcoin and the sidechain economy. Most importantly, by introducing tokens as an end-user incentive mechanism the BitHarvest Network allows miners to deepen mining engagement, drive incremental revenues, and participate in decentralized applications (DAPP).

The BitHarvest blockchain introduces **three main novel concepts:**

Safe mining combining PoW with PoC

This dual mining approach leverages the best of both PoW and PoC, utilizing the computational power and security of PoW while also incorporating the storage-based mining efficiency of PoC, resulting in a more sustainable and resource-efficient mining process.

Turing-complete BTH Virtual Machine (BVM)

the BTH Virtual Machine significantly enhances the blockchain's capabilities, enabling the execution of complex, smart contracts and decentralized applications. The BVM's Turing-complete nature ensures that it can run any computation given enough resources, paving the way for limitless innovation and flexibility within the BitHarvest ecosystem.

SHA256D + GHOST

This combined approach would aim to leverage the security strengths of SHA-256 and the efficiency and speed of the GHOST protocol. It would create a robust and fast blockchain network, aligning well with the goals of energy efficiency and rapid transaction processing in a Proof of Calculation (POC) framework. In a POC mechanism utilizing both SHA-256 and GHOST, SHA-256 could be responsible for the secure and immutable creation of new blocks through its hashing capabilities. Miners would use their computational power to solve SHA-256 hash puzzles, thus ensuring the security and integrity of the blockchain. The GHOST protocol, on the other hand, could be employed to enhance the throughput and efficiency of the blockchain. By incorporating some aspects of the GHOST protocol, such as considering stale blocks, the blockchain could potentially handle more transactions per second and reduce the likelihood of network congestion. This would be particularly beneficial for a system prioritizing rapid transaction processing and scalability.

This whitepaper will describe these concepts and the BitHarvest blockchain in detail. The Bitcoin sidechain, BitHarvest Network set to launched on BEP20-compliant tokens and will integrated in BitHarvest platform within 2024. The BitHarvest blockchain mainnet code will be released, and the first live mainnet implementation is planned to launch on 2025, at which time each BEP20 BTH token will be exchanged 1:1 for native BTH tokens.

	Pages
01. Safeguarding Bitcoin Miner Investments	4
02. The Need for a Bitcoin Sidechain, \$700 billion market	4
03. Background	5
04. Opportunity	6
05. BitHarvest Proof-of-Calculation (POC) protocol: securing Bitcoin and the sidechain	7
06. Terminology	8
07. BitHarvest Blockchain Ledger	10
08. POC Consensus Mechanism: Sharing your Calculation	11
09. Technology ingredients	12
9.1 Sidechain	12
9.2 Turing-complete smart contract layers	14
9.3 BTC Bridging: Two-way peg	15
10. Double Spending Detection and Penalty	16
11. A Single Currency System and Token Mechanics	19
12. Network architecture	19
13. BTH Features Comparison	20
14. Conclusions	21

01. Safeguarding Bitcoin Miner Investments

In April 2024 Bitcoin mining profitability margin will fall to less than 50% due to the decreasing block reward from 12.5 BTC to 6.25 BTC. Hundreds of millions of mining hardware will become instantaneously obsolete. This probably includes all mining machines in the market today, since two generations of chips (faster and with lower power consumption) will be developed and sold before 2025. Almost all current miners that have not replaced their hardware will see the end of their mining business. BTH, thanks to its PoC mining capabilities, gives these miners the opportunity to keep their business. Since BitBooster can mine both coins with zero marginal cost, miners will still be able to mine Bitcoin as long as the additional income provided by BTH mining compensates the profitability gap. Additionally, the reduction in mining profitability by the halving will create additional concentration in low-cost miners which will increase Bitcoin's network vulnerability. Hence, BTH could also play a key role in promoting a broad base of profitable miners, increasing the security and value of Bitcoin. Also, by starting today at a minimum cost, and creating applications for BTH, Bitcoin miners may not only protect their investment, but develop a whole new business opportunity.

02. The Need for a Bitcoin Sidechain, \$700 billion market

With a market valuation exceeding \$700 billion, Bitcoin remains a dominant force in the cryptocurrency market. Its underlying Proof of Work (PoW) technology has proven secure and stable. However, as the industry increasingly adopts smart contract capabilities, Bitcoin must evolve to maintain its competitive edge. Bitcoin sidechains offer a solution, providing a gateway to smart contract functionalities while preserving Bitcoin's core attributes.

Key Benefits of Implementing Smart Contracts via Bitcoin Sidechains:

Innovation Without Compromising the Main Chain

Sidechains are separate blockchains that are connected to the main Bitcoin blockchain. They allow for experimentation and implementation of new features, like smart contracts, without affecting the security and stability of the main Bitcoin network. This setup ensures that Bitcoin can explore new horizons in functionality without risking its foundational strengths.

Enhancing Bitcoin's Utility and Appeal

By leveraging sidechains, Bitcoin can support smart contracts, vastly expanding its utility beyond just a store of value. This added functionality can attract new users and

developers, keen on exploring decentralized applications (DAPP) and automated contracts in a Bitcoin-centric environment.

Increased Flexibility and Scalability

Sidechains can operate with different rules and features compared to the main Bitcoin blockchain. This flexibility allows for greater scalability, potentially handling more transactions at lower costs, a critical factor for the mass adoption of smart contracts.

Encouraging Decentralized Finance (DeFi) on Bitcoin

The integration of smart contracts through sidechains opens up the vast potential of decentralized finance (DeFi) within the Bitcoin ecosystem. Users can engage in lending, borrowing, and other complex financial activities in a decentralized manner, all underpinned by the robust security of Bitcoin.

Community Driven and Open to Innovation

Sidechains encourage a community-driven approach to development. They offer a platform for developers to propose and test new features, fostering an environment of innovation and continuous improvement within the Bitcoin ecosystem.

Maintaining Network Integrity and Security

One of the primary concerns of the Bitcoin community is preserving the network's security. Sidechains address this by allowing new functionalities to be added in a way that doesn't compromise the main chain's integrity, ensuring that Bitcoin remains secure and reliable.

03. Background

BitHarvest (the “company”) has been at the forefront of developing next-generation cryptocurrency mining boosting technologies. In a technology derived from traditional bitcoin mining, BitHarvest most recent technologies, “**HASH STRATEGY OPTIMIZATION**” and “**HASH AGGREGATION AND FILTERING**”, specifically addresses the problem of generating highly efficient bitcoin mining. The technology utilize machine learning (ML) and artificial intelligence (AI) to aggregate, analyse, filtering and provide strategy to the mining machine, thus optimizing the tradeoff on hashing efficiency.

04. Opportunity

Sidechain Mining

The company's mission is to leverage blockchain technology to create a Bitcoin sidechain and delivery network. In this network, Bitcoin miners are incentivized to share their redundant computing resources, addressing the current challenges of the Bitcoin blockchain. Utilizing the BitHarvest Virtual Machine (BVM), the BitHarvest Network acts as a "World Cache," composed of memory resources contributed by miners globally. Specifically, Bitcoin miners can purchase our BitBooster to serve as "caching nodes," thereby becoming sidechain miners. This role allows them to secure and operate the BitHarvest Network without compromising their existing hashing power.

Bitcoin Sidechain

The sidechain operates in tandem with the main Bitcoin blockchain, designed for interoperability to ensure seamless transactions between the two. This symbiotic relationship facilitates the transfer of assets and data, maintaining a secure and consistent ledger across both chains. The sidechain enhances the functionality of the Bitcoin ecosystem while being secured by the robust framework of the main Bitcoin blockchain.

06. Terminology

Address/Wallet

In the BitHarvest network, an address or wallet is created through a pair of keys comprising a private and a public key. The public key, derived algorithmically from the private key, is used for various purposes such as encrypting session keys, authenticating signatures, and encrypting data decryptable by the private key.

Application Binary Interface (ABI)

This refers to the interface that facilitates communication between two binary program modules, typically involving a library or system software and a user-run application.

Application Programming Interface (API)

APIs are critical for the development of user clients. They enable the creation of token issuance platforms by developers.

Asset/Token

Within the BitHarvest documentation, the term 'asset' is synonymous with 'token'.

Block

A block in the BitHarvest blockchain is a digital ledger of transactions, including components like a magic number, block size, block header, transaction counter, and the transactions themselves.

Block Reward

Rewards for block production are allocated to a specific sub-account (address/wallet).

Block Header

Part of the block structure, the block header in the BitHarvest blockchain includes several elements like the hash of the preceding block, the Merkle root, a timestamp, version number, and witness address.

Cold Wallet

This type of wallet, also known as an offline wallet, stores the private key without any network connection, ensuring enhanced security. Typically installed on devices that remain offline, cold wallets are crucial for the secure storage of the BTH private key.

Decentralized Application (DAPP)

DAPP operate independently of any centralized authority, facilitating direct interactions or agreements between end-users or resources without intermediaries.

gRPC

An open-source system for remote procedure calls, initially developed by Google. It employs HTTP/2 for transport and Protocol Buffers as its interface language, supporting features like authentication, streaming, and more. gRPC enables the generation of cross-platform client and server bindings in multiple languages.

Hot Wallet

Contrary to cold wallets, hot wallets (or online wallets) keep the user's private key accessible online, which may expose them to potential security threats.

Java Development Kit (JDK)

This kit is essential for Java application development and comprises both the Java application environment and various Java tools.

Merkle Root

In blockchain technology, this term refers to the combined hash of all transaction hashes in a block.

Remote Procedure Call (RPC)

This computing process allows a program to execute a procedure in a different address space, appearing to the programmer like a local procedure call.

Scalability

A characteristic of the BitHarvest Protocol, indicating the system's ability to handle increased workload or expand in response to growth.

BTH

The native cryptocurrency of the BitHarvest network, functions as its primary transactional medium.

07. BitHarvest Blockchain Ledger

The BitHarvest ledger is a decentralized ledger designed for the Bitcoin economics. It powers the BitHarvest token ecosystem which incentivizes Bitcoin miners with BitBooster to share their redundant hash resources, and enables them to engage more actively with DAPP and Bitcoin mining. To realize these goals, a number of challenges, many of which are unique for Bitcoin mining applications, need to be tackled.

One of such challenges is to support ultra high transaction throughput. Although many blockchain projects are facing transaction throughput problems, scaling for sidechain is different and possibly even more complex. Typically, a traditional financial segments are capable of processing anywhere between 1500 and 2000 transactions per second. This makes them much more efficient than Bitcoin and Ethereum, as well as many other cryptocurrencies.

The integration of DAPP with a sidechain like BitHarvest presents a unique set of challenges. It involves ensuring seamless interoperability between the main Bitcoin blockchain and the BitHarvest sidechain. The goal is to create a sidechain that is not only efficient and secure but also capable of supporting a diverse range of DAPPs **without compromising the performance or security** of the main blockchain.

Transferring Bitcoin (BTC) to a sidechain is a critical functionality for BitHarvest, but it comes with its own set of hurdles. The process must be secure, transparent, and efficient. This involves creating a reliable mechanism for locking BTC on the Bitcoin blockchain and then issuing corresponding tokens on the BitHarvest sidechain. This mechanism must **prevent double-spending** and ensure that the integrity and value of BTC are preserved during the transfer.

Security is paramount in any blockchain project, and for BitHarvest, **safeguarding against a 51% attack is critical**. A 51% attack occurs when a single entity gains control of more than half of the network's mining power, potentially allowing them to manipulate the blockchain. For a sidechain, this risk could be even more pronounced due to potentially lower levels of mining and validation activity compared to the main chain.

We note that the sidechain must implement robust security protocols to mitigate this risk, ensuring the integrity and trustworthiness of its sidechain. This could involve innovative consensus mechanisms, enhanced validation processes, and continuous monitoring to detect and prevent any malicious activities.

08. POC Consensus Mechanism: Sharing your Calculation

Alice activates 1 BitBooster and aims to earn both BTC and BTH. Initially, she enters into a Bitcoin mining contract by sharing his BitBooster's calculation to increase the efficiency of the mining machine. This earns her BTC as a reward for discovering a new Bitcoin block. Concurrently, Alice contributes to securing a BTC sidechain by utilizing BitBooster's hash aggregation capability to operate nodes within the BTH network's nodes. In recognition of her role in securing the network, she is rewarded with BTH tokens.

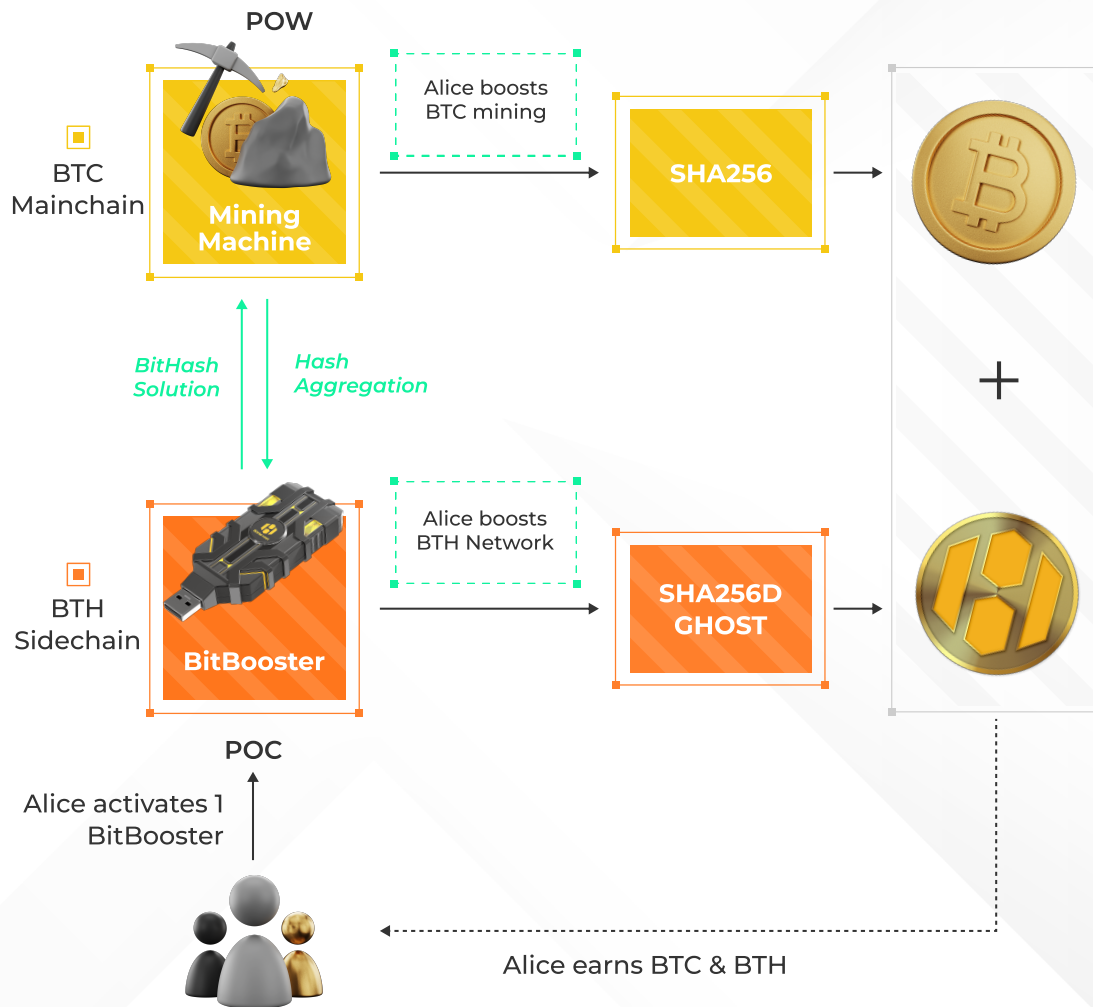


Figure 2: POC workflow.

09. Technology Ingredients

The following are the key ingredients which enable the protocol functionalities described in Section 8, and overcome the challenges described in Section 7. BTH platform is at its core, the combination of: Sidechain, Turing-complete smart contract layers, and Bitcoin bridging.

9.1 Sidechain

A sidechain is a unique blockchain that is connected to a parent blockchain mechanism. This innovative linkage enables the secure of BTH blockchains. BTH blockchain is designed to complement and interact with the Bitcoin network.

Zero-knowledge proofs

One of the most innovative aspects of our BTH blockchain is its ability to interact seamlessly with the BTC network, particularly through a technique known as zero-knowledge proofs. This method enhances the connection between BTH and BTC, providing a robust framework for blockchain entanglement.

A zero-knowledge rollup (zk-rollup) is a sidechain solution that moves computation and state off-chain into off-chain networks while storing transaction data on-chain on a mainchain network (for example, Bitcoin). State changes are computed off-chain and are then proven as valid on-chain using zero-knowledge proofs.

Zk-rollups is a cryptographic method that mathematically verifies transaction without exposing their contents. This approach inherently minimizes the risk of fraud, as transactions are validated through stringent mathematical proofs, bolstering the securities against manipulation.

This method greatly increase transaction throughput and help reduce transaction costs while inheriting the security of the mainchain network they are connected with for settlement. Instead of posting every single transaction on mainchain, zk-rollups only have to periodically post valid batches of transactions from the sidechain network bundled up to the mainchain, effectively only leveraging the censorship resistance and security of the base layer for transaction settlement. Rollups also commonly use data compression mechanisms to reduce the amount of data posted on the mainchain.

Zk-rollups increase scalability as instead of having to post all transaction data on-chain, they only need to periodically provide valid bundled-up transaction batches that are executed using off-chain computation. These bundles are then “rolled up” into one summary of the state changes that are verified by the base layer using a validity proof that proves the correctness of the changes using a zero-knowledge proof, demonstrating with mathematical certainty that the state changes proposed by the sidechain are correct and are the result of the execution of the given batch of transactions. Zk-rollups typically rely on the base layer for data availability, settlement, and censorship resistance.

BitHarvest Network utilize the combination of a sovereign rollup (aka client side validation), recursive ZK proofs and a forced transaction mechanism using inscription-like envelopes.

Forced Transaction Envelopes

```

OP_FALES
OP_IF
  OP_PUSH “bthrollup” --à tag for rollup
  OP_PUSH 1
  OP_PUSH “forced-txn” --à tag for operation
  OP_PUSH 0
  OP_PUSH “0001.....” --à serialized txn
OP_ENDIF
    
```

To fully leverage Bitcoin's security in client-side validation, it's vital to ensure the recursive nature of our proof system and the completeness of all prior proofs on the data availability layer of Bitcoin. Light clients rely on this for accurately determining the state's correctness and completeness, tracing back to the genesis. Each Bitcoin block feeds into the rollup state, verified through a mechanism known as ‘ValidityCondition’, which checks consecutive block headers. This process ensures the comprehensive scanning of Bitcoin blocks and the validation of proofs, tightly integrating our rollup proofs with Bitcoin headers.

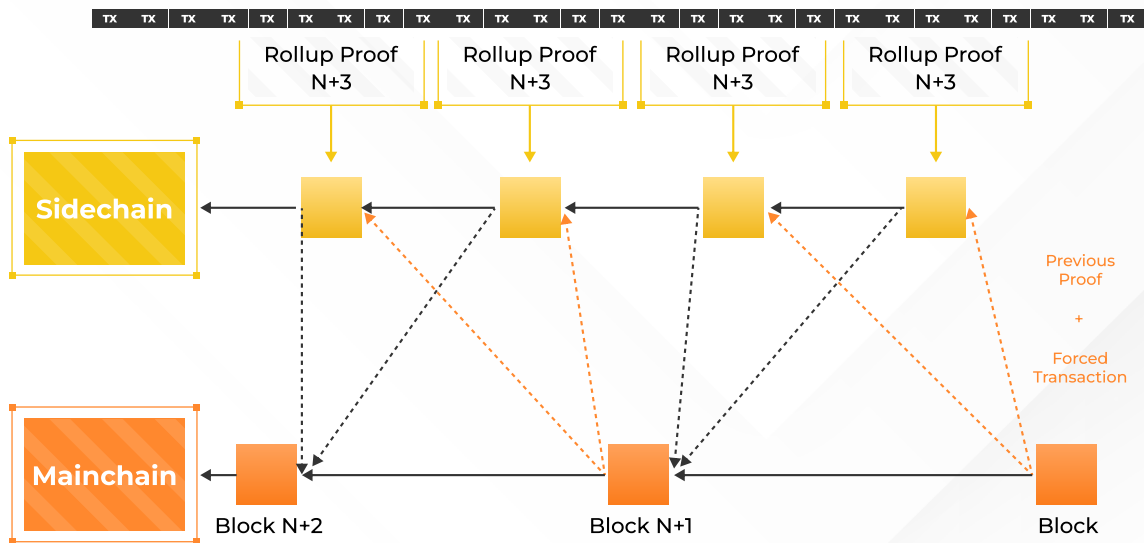


Figure 3: Sidechain's zero-knowledge proof.

Our strategy underscores the importance of staying abreast of blockchain advancements and pushing the limits of what's achievable. By implementing inscription-like envelopes, we ensure that our zk-rollups inherit Bitcoin's censorship resistance. The integration of zero-knowledge proofs, Bitcoin technology, and rollup advancements has enabled the creation of a zk-rollup mechanism fully secured by Bitcoin. Our goal is to expand the Bitcoin user base by offering fast, low-cost financial applications secured by the most valued block space in the cryptocurrency realm, Bitcoin.

9.2 Turing-complete smart contract layers

BTH virtual machine (BVM) offers a smart contract runtime environment **fully compatible with Ethereum Virtual Machine (EVM)**. It provides full-fledged support for Turing-complete smart contracts. Solidity-based Ethereum smart contracts can be ported to the BitHarvest Ledger with little effort. Solidity has grown a large developer community and the prospect of allowing that proven talent pool to also contribute to BitHarvest without reinventing the wheel was a prime consideration in enabling compatibility with the EVM.

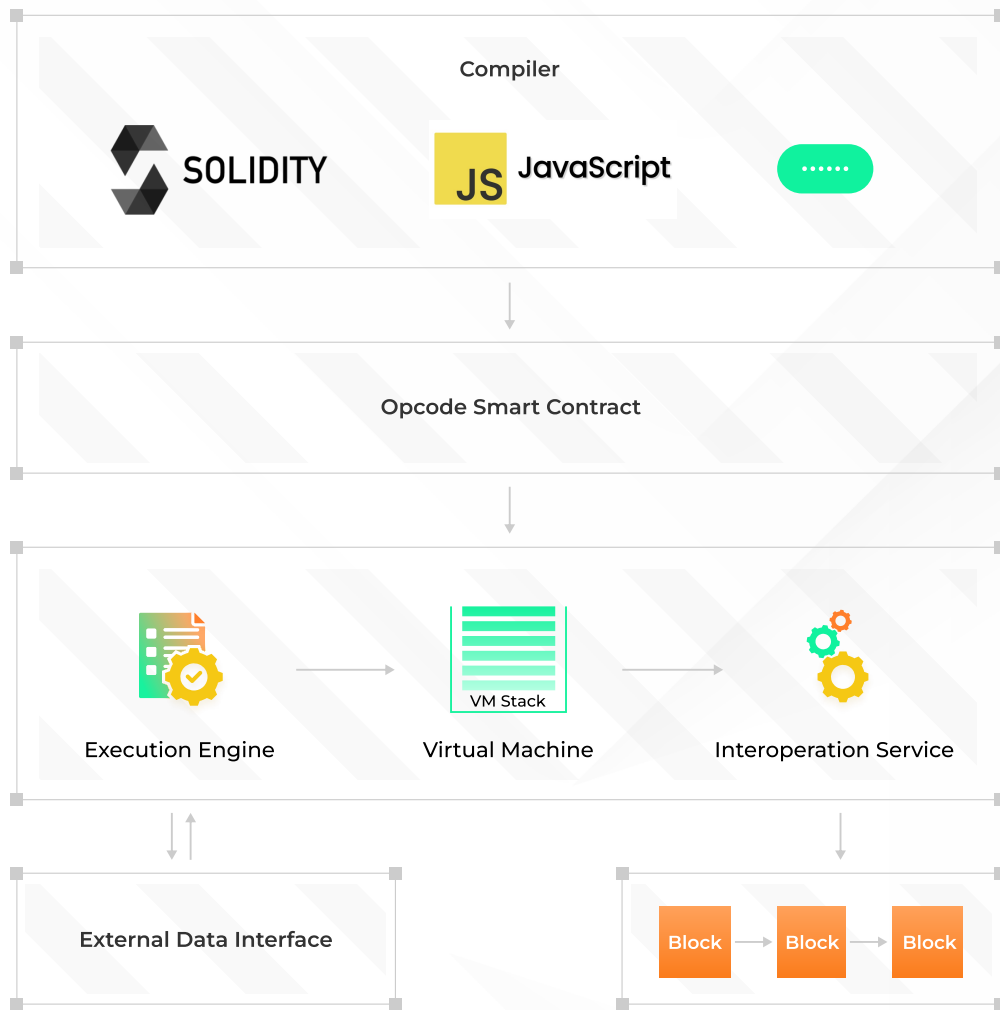


Figure 4: BVM Workflow

9.3 BTC Bridging: Two-way peg

A sidechain is a distinct blockchain that operates independently but has its native currency value pegged to another blockchain's currency. This pegging is achieved automatically through proofs of payment, facilitating a two-way peg system where two distinct currencies can be exchanged freely and automatically without the need for price negotiation.

To bridge Bitcoin's BTC to BTH Network's BTC, BitHarvest implement two-way pegged mechanism. The process of exchanging BTC for BTC in BTH does not involve a direct transfer of currency between the two blockchains in a single transaction. This is because the Bitcoin blockchain cannot verify the authenticity of balances on another blockchain.

Instead, the exchange process works as follows:

When BTC is exchanged for BTC in BTH, an equivalent amount of BTC is locked on the Bitcoin blockchain. Simultaneously, the same amount of BTC in BTH is unlocked or made available in BTH Network.

Conversely, when converting BTC in BTH back to BTC:

The corresponding amount of BTC in BTH is locked in the BTH blockchain. An equivalent amount of BTC is then unlocked in the Bitcoin blockchain.

This mechanism ensures a seamless and secure exchange between BTC and BTC in BTH, allowing users to leverage the functionalities of BTH while maintaining the value and stability associated with Bitcoin.

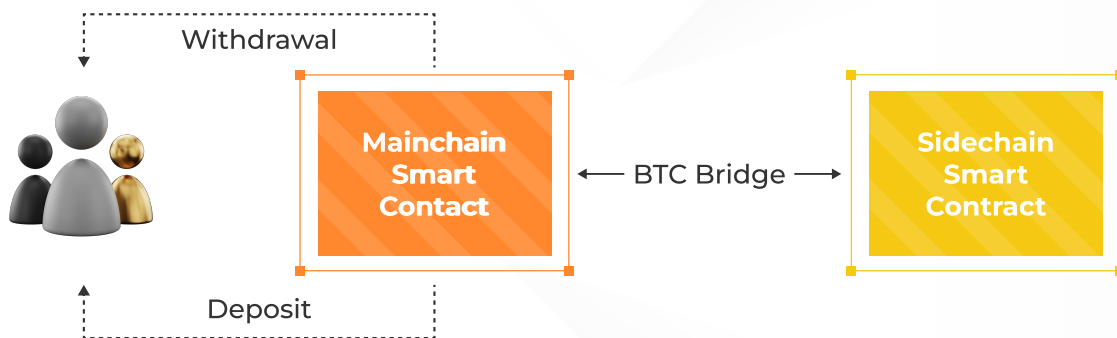


Figure 5: Bitcoin Bridging Overview

10. Double Spending Detection and Penalty

To safeguard the integrity of the BTH blockchain, particularly within its BTC bridging system, a robust mechanism is essential to detect and penalize double spending attempts. This mechanism ensures that any user, let's call her Alice, is deterred from malicious activities due to the economic disadvantages of such actions.

Detection of Double Spending

Miners on the BTH network actively monitor all on-chain transactions within the bridging system. If Alice attempts to double spend, it would be detectable when the deposit in her bridging collateral cannot cover a consolidated payment transaction that she and another peer have signed.

Penalizing Double Spending

To deter Alice from double spending, the system ensures that her net gain from such an act is negative. This is achieved by requiring Alice to place a collateral that is greater in value than her deposit in the bridging collateral. In a scenario where double spending is detected, the full amount of Alice's collateral is forfeited, leading to a net loss.

Scenario Analysis

Consider a case where Alice colludes with a malicious peer, say Edward. Alice might attempt to manipulate the system by sending her entire deposit to Edward, who then quickly settles the transaction. Even if Alice temporarily gains the resource for free, once her double spending is detected (as honest peers like Bob, Carol, or David commit their transactions), her entire collateral is lost. Therefore, Alice's net gain (net_{Alice}) from double spending is calculated as the deposit minus the collateral.

$$net_{Alice} = deposit - collateral$$

As long as the collateral is greater than the deposit, Alice's net return is negative, making double spending economically unviable. The system's design is such that Alice, if rational and profit-motivated, has no incentive to engage in double spending, as it would always result in a net loss.

In cases where Alice is honest but faces malicious peers, the bridging system is structured to minimize her loss.

This double spending detection and penalty mechanism for the BTH blockchain effectively deters fraudulent activities by making them economically disadvantageous.

Through vigilant monitoring, collateral requirements, and a strategic incentive structure, the BTH network maintains its integrity and trustworthiness.

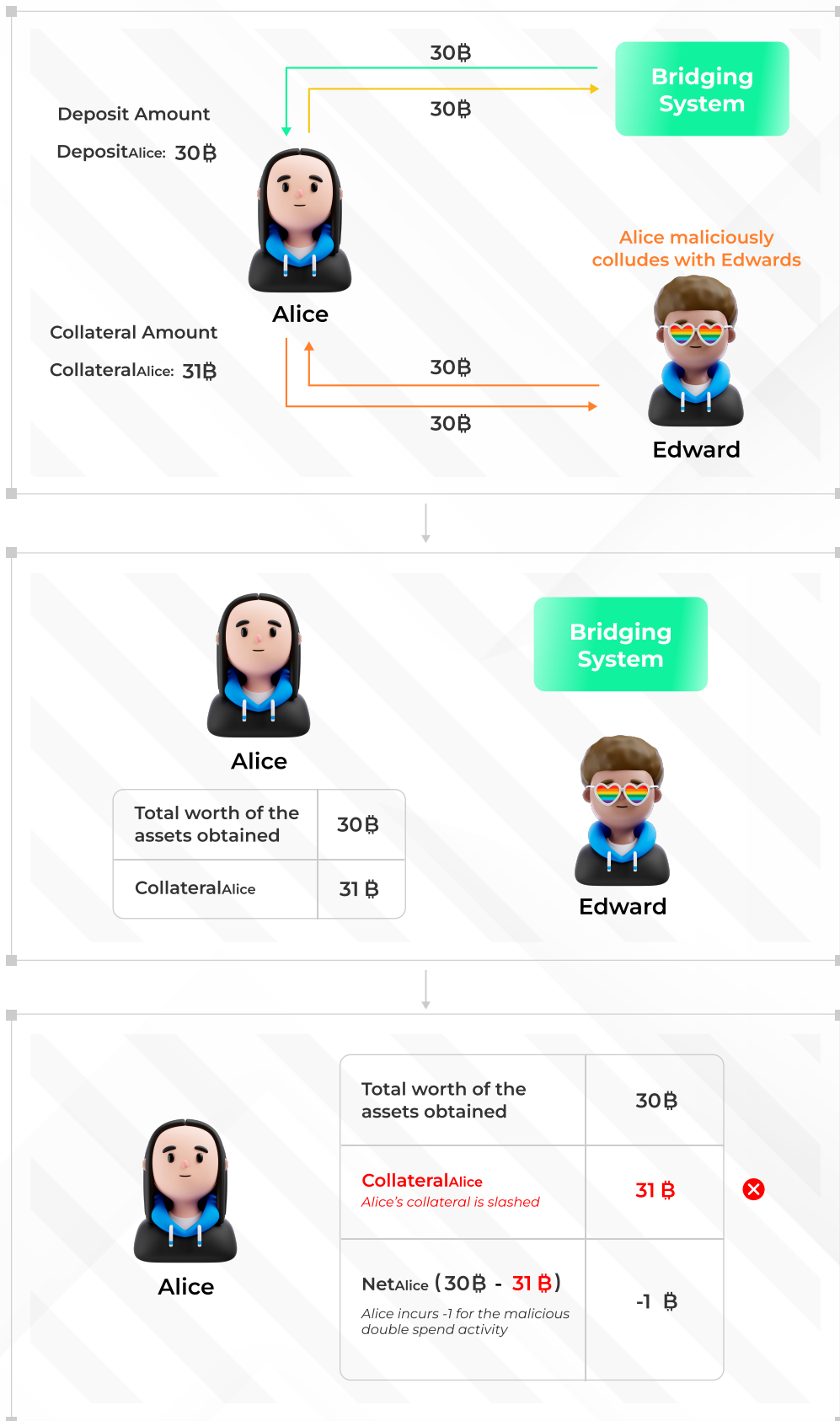


Figure 6: Malicious Actor Detection and Penalty shows malicious actor Alice attempting to make a double spend and the resulting penalty she receives.

11. A Single Currency System and Token Mechanics

In the interest of securing the network, installing simplicity and stability, and increase the digital store of value, the Biitharvest blockchain will use a single currency system. The BitHarvest token will be used to activates BitBooster, used as the 'gas' to pay transaction fees, and used as the native transaction currency in the BitHarvest ecosystem.

Initial as an BEP20 token, the BTH token supply is currently fixed at 21 million. At Mainnet launch, each holder of the BEP20 BTH token will receive native BTH tokens on the new blockchain on a 1:1 basis. The supply of native BTH on the new blockchain will also be permanently fixed at 21 million, meaning no new BTH tokens will ever be created.

The primary reason for fixing the BTH token supply is to make it prohibitively expensive for malicious actor to acquire enough tokens to threaten the network. Since new BTH tokens will never be created, the only way to acquire more is by purchasing existing tokens and over time making it more expensive to amass a controlling amount of BTH tokens.

12. Network architecture

Based on the above primitives, the core infrastructure of the Bitcoin sidechain protocol is a control plane between Bitcoin and the BTH Network. This control plane is responsible for various key functionalities, including provide Bitcoin timestamping service to the BTH network to enable their synchronization with the Bitcoin network, and act as a market place, match Bitcoin mainchain and the BTH blockchain.

The control plane is implemented as a chain to make sure that it is decentralized, secure, censorship resistant, and scalable. For example, Bitcoin network's limited and expensive block space makes it unsustainable and unscalable for every blockchain to directly timestamp on to it, which hinders the adoption of Bitcoin utility. To solve this problem, the BitHarvest team has designed a secure Bitcoin timestamping protocol and implemented it as a BitHarvest Virtual Machine (BVM).



Figure 7: System architecture with control and data planes

13. BTH Features Comparison

We attempt to compare BTH with other blockchains, and we show that essentially BTH present better technical choices without eroding decentralization, where decentralization is measured as the inverse of the cost of running a full-node instance.

			
Item	Bitcoin	Ethereum	BTH
Average Confirmation Time	10 min.	12 sec (GHOST)	10 sec. (GHOST)
Turing complete Smart-Contracts	No	Yes	Yes
Adds value to Bitcoin	-	No	Yes (Bridge & POC mining)
Security guarantee	SHA256D miners	Proof of Stake (POS)	SHA256D + POC miners
Scalability [tps]	3 to 24	Unbound	10,000 at launch
Native Token	BTC	ETH	BTH
Tokenomic	Deflationary	Deflationary	Deflationary

Table 1: Blockchain comparison between BTC, ETH, and BTH.

14. Conclusion

Bitcoin is the first and still the top blockchain in terms of market capitalization. However, beyond a store of value, its utility has been limited by its small blockspace, high latency, and limited programmability. BitHarvest stands at the vanguard of blockchain innovation, ingeniously leveraging the robust infrastructure of Bitcoin to expand its capabilities far beyond a mere store of value. Our works represents a paradigm shift, integrating advanced POC mechanisms for SHA256D+GHOST security and employing cutting-edge, modular protocols that transcend Bitcoin's traditional constraints. At its core, BitHarvest enhances Bitcoin's utility, enabling it to secure and empower diverse blockchain applications while maintaining a fine balance between technical sophistication and user accessibility. This approach not only addresses the limitations of Bitcoin's block space, latency, and programmability but also fosters a renaissance in Bitcoin's ecosystem, setting the stage for future creative applications. As a visionary reinterpretation of Bitcoin's potential, BitHarvest is a testament to the evolving nature of blockchain technology, driving forward a narrative of innovation and versatility, and positioning itself as a key player in the transformative journey of the blockchain domain.