Botanix protocol: An EVM equivalent Layer 2 on Bitcoin

info@botanixlabs.xyz

Abstract. Since the launch of the Bitcoin whitepaper [1], there is no clarity yet on how the future crypto infrastructure will look like. Multiple new blockchains and smart contract programming languages with respective application ecosystems have emerged. Different properties like composability, speed, privacy and decentralization each play a role. However, we argue that the most important property that underlies any of the others is decentralization. On a long enough timeline, all other properties are lost if a trusted third party is required. Bitcoin as a base layer is optimized to be as decentralized and secure as possible. This makes it suited as a global reserve currency but comes with tradeoffs like composability and scalability. While the lightning network [2] shows very promising results to solve for instant and free payments, the question remains on how to bring smart contracts to Bitcoin.
Ethereum has seen a massive growth in decentralized finance applications that are mostly unavailable on Bitcoin. The total value on the second layers of Bitcoin is less than 0.1% of the market cap of Bitcoin while at the same time the value of wrapped Bitcoin available on Ethereum is higher than 2%. Bitcoin has not seen the massive growth in TVL (Total value locked) on its second layers or in its applications.

This paper proposes a second layer built on top of Bitcoin with full Ethereum Virtual Machine (EVM) equivalence. With Bitcoin as the most decentralized and secure bottom layer, the second layer will open the doors to the composability, ecosystem and capabilities of Ethereum smart contracts. We introduce the Spiderchain primitive, a second layer design on top of Bitcoin that is optimized for decentralization.

Versions and Revision History

Date	Description
Sep 26, 2023	Small corrections.
	Added catching and reporting of malicious attacks.
June 17, 2023	Small corrections.
March 25, 2023	Initial version.

Contents

1 Introduction

Bitcoin is the largest and most well-known cryptocurrency, known for its decentralized structure and blockchain technology. While decentralization has many benefits, such as increased security and censorship resistance, it also comes with limitations like smaller block sizes and slower transaction times. To fully utilize Bitcoin's potential as a decentralized global currency, new protocols and solutions may be necessary to address these challenges and enable wider use of Bitcoin for financial products and applications.
Ethereum introduced a blockchain with a Turing complete programming language [3] on its parent chain. Its composability has produced an ecosystem of decentralized applications challenging the scalability of the base layer. The Ethereum Foundation's vision for solving the scalability problem consists of EVM (Ethereum Virtual Machine) compatible chains layered on top of each other. The Ethereum parent chain will serve as a settlement layer at the bottom. The most secure and decentralized chain is required as a foundational layer in a layered future. Ethereum still faces centralization questions with multiple hard forks on the roadmap, the role of the Ethereum Foundation, the centralizing move to Proof-of-Stake and the OFAC sanctions as the biggest examples.

Different technologies for constructing a second-layer on Bitcoin already exist. Examples of these include state channels, drivechains, multisig rollups, and Bitcoin soft-fork proposals which could enable ZK and optimistic rollups. The Lightning Network (state channels) and Liquid (a multisig federation) are successful second-layers that are already in production. In the following section, we will provide a more in-depth overview of the current Bitcoin second-layer ecosystem and the compromises that come with each.

In this paper we propose **the Botanix protocol**. Botanix is a solution for a decentralized chain built on top of bitcoin that uses the fundamentals of Lightning for decentralization to run an Ethereum Virtual Machine. Botanix is an account-based model (like Ethereum), instead of the UTXO (unspent transaction output) model of Bitcoin. The current state of Botanix is then a list of the account balances and smart contracts. Each Botanix full node will run Bitcoin core and the Botanix protocol.
Botanix will use synthetic BTC as the native currency which is 1:1 pegged with Bitcoin, or in other words every synthetic BTC represents one Bitcoin. The consensus protocol consists of a Proof-of-Stake (PoS) model with slashing. While the benefits of Proof-of-Work are indispensable for the base layer of Bitcoin (no ownership centralization over time and during initial coin distribution), for a second-layer built on top that is pegged to BTC, the same argument no longer holds and the speed and performance benefits of PoS outweigh the downsides. Since synthetic BTC, the native currency of Botanix is pegged 1:1 with Bitcoin, the total block reward for stakers does not have a fixed fee. Instead, the reward will consist of multiple items (see section 4.5 Block Reward).

2 Design Rationale

The design of Botanix is focused on designing a missing piece in the crypto infrastructure. The crypto ecosystem is fractured in what can be broken down into three technological battles. The reality is even more complex but for the sake of making sense of the ecosystem, most infrastructure designs can be put into these three battles. We will look into each of these battles, reduce it to their respective first principle and use these fundamental assumptions as the design choices for Botanix. The first section below provides a deeper analysis of each battle.

2.1 Technology battles in crypto

The Layer 1 decentralization battle: Bitcoin

On the bottom layer many chains have been designed and optimized for different properties. During the blocksize war we have seen a real-life battle between de-bottlenecking Bitcoin (large block size camp) and the more ideological point of view to optimize for decentralization and reduce centralized power in the ecosystem. One can extrapolate from there what might happen to the broader ecosystem. Therefore decentralization as a property underlies all the other properties. As the value and adoption of a certain chain grows, the chain comes under more scrutiny from governments or parties that have an interest in changing or having control in the chain. If a chain is not decentralized, this results in a possibility of losing the properties it first gained value from.
From another point of view, many arguments have been made by people in the Ethereum ecosystem for a future built in layers on top of each other [9]. When most of the transaction space on the Ethereum parent chain is taken up by settlements of different rollups, Ethereum will become a global settlement layer. However, in a layered future where the bottom layer solely provides settlement, there is no need for additional functionality like smart contracts that might endanger security or decentralization. In fact, in a layered world where the bottom layer becomes a settlement layer, it makes sense that it has to be the most decentralized and secure layer 1 there is.
Therefore Bitcoin is chosen as a base layer. The most decentralized and secure blockchain is the best suited to be the settlement layer.

Scalability battle: Layered

After the launch of Bitcoin, it became clear that it is impossible to achieve all three elements needed in a blockchain called the blockchain trilemma: Security, Decentralization and Scalability. To solve for scalability, there are two main theories. A multi-chain world theory consists of multiple layer 1 chains optimized for different properties. In contrast to this stands a layered approach where blockchains are built on top of each other and

security properties are inherited from each other.
In order to make sense, we have to go back to the basics. In cryptography there is an overall guiding principle of simplicity. The more complex an algorithm, the more possible attack vectors and the harder it is to prove security. Complex protocols often seem secure because it is harder to grasp the full design. This is however not a lasting security design choice. Security through obfuscation only lasts as long as a party is able to hide its security design.
A multi-chain world could have a layer for speed, another for privacy and others for composability. Between these layers, entities can bridge from one chain to another. The incredibly difficult problem here is to make a cryptographically secure bridge from one chain to another. This design means that every bridge and every layer one on its own has to be cryptographically secure. Even then, every interface of bridge and parent chain has an opportunity for attackers to attack. Timing issues, forgeries and pricing oracles are some of the big issues that arise in a multi-chain world.
A layered approach provides less complex designs and as a result less security assumptions. Every layer can be optimized for different aspects like speed, security and others. The beauty of cryptography and security inheritance ensures that upper layers inherit some or all of the security aspects of lower layers.
Besides bringing smart contracts to Bitcoin, the security inheritance of a layered approach is the main reason Botanix builds a second-layer on top of Bitcoin.

The smart contract language battle: Ethereum

The Ethereum Foundation has led the way as a composable smart contract blockchain. It developed a new smart contract programming language called Solidity. Ethereum has created an ecosystem and achieved a big head start regarding the number of applications and developers.
After Ethereum, multiple layer one chains have optimized for different properties in their choice of programming language. For example, Solana has made the design choice to go with Rust. This enables Solana to attract the software engineers already familiar with the Rust programming language to develop in the Solana ecosystem.
Also in the layer two ecosystem different chains have chosen to optimize for different reasons. For example starkware (ZK Rollup on Ethereum) has opted to design a new programming language Cairo.
Overall the programming language battle is fought in terms of composability, ecosystem and transportability. While composability in the newer chains might be bigger, there is a head-start of an ecosystem of (proven) applications that will be difficult to beat. Especially because of the associated dollar amounts on-chain, Solidity smart contracts benefit from the Lindy effect and experience a higher trust level of security.
From a programming language perspective, Solidity seems to have set a stronghold in the crypto world and Botanix has therefore opted to build an EVM.

2.2 Consensus: Proof-of-Stake

Proof of Stake (PoS) is a consensus model which employs a staking mechanism to secure the network. Participants in the consensus are required to stake a monetary value in order to create new blocks. On the other hand, Proof of Work (PoW) is a consensus model in which miners must complete a certain amount of computational work to create a new block. PoW has been shown to facilitate a fair initial distribution and a trend toward decentralization. All participants in PoW (the miners) must spend money on real-world energy bills, resulting in a trend toward reduced participation share of the miners in the network. Conversely, PoS has a tendency towards centralization, as stakers in PoS receive rewards in the native currency, thus eventually leading to a larger participation share of the network for the stakers.
Botanix has opted for a Proof of Stake consensus model. Since Botanix will be 1-1 pegged, the centralization trend for the participants seen in PoS will be counterbalanced by Bitcoin's PoW and Botanix can benefit from Bitcoin's initial fair distribution. However, this also means there will be no base fee reward for the stakers and the fees gathered by the staking participants stand against the opportunity cost of locking their stake. See also the section 4.5 for a deeper analysis of the block reward. Proof of Work makes a lot of sense for the base reserve currency due to its decentralization trend and fair distribution, while the performance and speed benefits of Proof of Stake make more sense for a pegged second-layer.

2.3 Bitcoin second-layers and sidechains

There are various layer 2 technologies that offer distinct benefits and features. Examples of layer 2 technologies on Bitcoin include the Lightning Network, which utilizes state channels for efficient and cost-effective payments, and the Liquid Network, bringing composability to a layer 2 built using a federated multisig. These solutions improve the speed, composability and user experience of blockchain networks. However, there are also challenges and limitations, such as the liquidity and liveness requirements for the Lightning Network or the centralized nature of the federated multisig in Liquid. In the next section we introduce the Spiderchain primitive, leveraging the composability of Liquid and the decentralization of the Lightning Network. The Spiderchain is a decentralized chain of multisigs opening up Bitcoin to composability.
Here we look at the different tradeoffs of the lightning network, a federated multisig solution and validity rollups (eg ZK) in more detail.

The Lightning Network

State channel rollups like the Lightning Network operate by creating a "state channel" between two parties. It is a peer-to-peer funded payment channel that allows them to exchange information and transact with each other without needing to broadcast every

transaction to the blockchain. Once the channel is open, virtually free and instant micropayments are possible. The network has a trustless structure by using time locks. When closing the channel, the final result of the transaction is recorded on the blockchain. Additionally, state channel rollups provide a high degree of privacy, as the transactions within the state channel are not visible to the rest of the network.

On the downside, the setup requires users to provide a lot of liquidity. Opening a state channel means funding it with capital with an associated opportunity cost. Another downside is the liveness required for all the participants in the network.

UTXO vs Account model. Another limitation is that Bitcoin uses an UTXO model compared to Ethereum's account model. Because of the state and the number of different potential outputs of a smart contract that's possible on an account model like Ethereum, it is hard to map this onto an unspent output model like Bitcoin and its Lightning Network. Therefore Botanix separates the two and considers the Spiderchain the full collateral of the Bitcoin available on the Botanix EVM. The total amount of Bitcoin on Botanix equals the total amount of Bitcoin locked in the multisig network.

Federated multisig

One way to separate the Bitcoin the 'asset' and Bitcoin the blockchain is to keep all the Bitcoin of the 2nd layer in a wallet (secured by a multisig) that is in control of a federation (eg. 15 independently chosen guardian). That federation can then run a new blockchain that brings new properties. An example of this on Bitcoin is Liquid [4] which uses a federation to control the pegged sidechain.
While this design can massively improve the properties like speed, composability or privacy, the risk is the trust required in this federation.

Optimistic and Validity rollups

There are two types of rollups: optimistic rollups and validity rollups (also known as "zk-rollups"). Optimistic rollups use fault proofs to ensure that state transitions are valid, while validity rollups use validity proofs. Validity rollups are considered 'trustless' because they use cryptographic validity proofs to prevent invalid state transitions and withdrawals, and do not require any additional trust beyond the trust assumptions of the base layer (L1).
They are similar to other layer 2 blockchains in that they allow multiple transactions to be bundled together and processed off-chain, reducing the amount of data that needs to be recorded on the parent blockchain itself. Similar to multisig layer 2 blockchains, rollups allow any user on the network to participate.

Bitcoin BIPs. For ZK or Optimistic Rollups to work natively on Bitcoin, a BIP (Bitcoin Improvement Proposal) would be needed [7]. With additional opcodes a validity rollup could work if you added two main primitives to the design: validity proof verification and recursive covenants [8].

Decentralization path of ZK and Optimistic rollups. The layer 2 developments on Ethereum have gained significant attention because of the strong cryptographic security primitives. However, the setups of ZK and Optimistic rollups require a validating smart contract on the Ethereum parent chain. This smart contract is controlled by a single party (eg Optimism, Arbitrum or Starkware). This presents an attack vector and a challenge for long-term decentralization. See L2Beat.com for an extensive overview [6]. One solution for decentralizing the validating contracts is to have multiple entities run their own versions of the smart contracts that provide validity proof. This future of decentralized multisigs/smart contracts is similar to the primitive of the Spiderchain. The Spiderchain is however not limited to the performance limitations put forth by validating zero-knowledge proofs and can enjoy the full performance of the EVM.

Summary

In summary, the Lightning network provides a decentralized layer 2 technology but suffers from liquidity, liveness and Bitcoin's UTXO restrictions. Federated multisigs and optimistic/validity rollups provide the composability and flexibility to bring new properties but suffer from centralized attack vectors.

3 Botanix Protocol

Some definitions are below to avoid any future confusion.

Definition 1. Parent chain. The parent chain, layer 1 or first blockchain refers to Bitcoin.

Definition 2. Peg-in. The process of lifting Bitcoin from its parent chain to Botanix chain.

Definition 3. Peg-out. The process of unlifting Bitcoin from Botanix chain to the Bitcoin parent chain.

Definition 4. Layer 2. A layer 2 is a secondary protocol built on top of an existing blockchain system to provide additional properties.

Definition 5. synthetic BTC. Synthetic bitcoin refers to native coin used on the Botanix EVM chain that represents BTC. All the synthetic bitcoin in the Botanix EVM equals the bitcoin on the Spiderchain.

Definition 6. Multisig Multisig (short for multi-signature) is a type of technology that requires more than one user to sign off on a transaction before it can be completed. The multisigs in Botanix will require a 2/3rd majority.

Definition 7. Orchestrator nodes. A node runner, liquidity source of the Botanix chain. An Orchestrator will run the Spiderchain, the EVM and Bitcoin. It is responsible for the Botanix operations and provides liquidity both on the Bitcoin side as on the Botanix side. *Orchestrator nodes* participate in the Spiderchain and are the only entity able to construct new blocks, mint and burn synthetic BTC. The *Orchestrator nodes* need to put in a stake in order to participate.

Definition 8. Stake The mechanism where Bitcoin is held in collateral to ensure honest *Orchestrator node* operation. In case of malicious operation, the Bitcoin stake will be slashed. The stake can be kept in a fidelity bond, a separate multisig among Orchestrators.

The Botanix protocol is a second-layer Ethereum Virtual Machine (EVM) built on top of Bitcoin. Botanix is a PoS (Proof-of-Stake) on Bitcoin, where you stake physical Bitcoin on Bitcoin to secure the second layer. The whole protocol runs on Bitcoin. It allows users to use Bitcoin natively in any of the applications built on an EVM. The Layer 2 protocol is optimized for decentralization and allows anyone to participate and run a full node. The actual Bitcoin on Botanix will be locked in the Spiderchain, a series of consecutive multi-sigs that are controlled by a random subset of *Orchestrator nodes*. The stake or collateral provided ensures honest participation. Therefore, moving from the Bitcoin parent chain to

the Layer 2 includes one additional trust assumption: no single party has majority control of the stakerset. The Botanix protocol can be implemented on Bitcoin today, without the need for any BIPs (Bitcoin Improvement Proposals).
The Botanix network provides additional functionality by bringing smart contracts that are not possible on Bitcoin. While the Bitcoin parent chain optimizes for decentralization and security, the second layer network optimizes for bringing the complex parts off-chain. The idea is a Lightning Network style of node operators that ensure the correct state of the Botanix blockchain. Since this second layer network operates as a blockchain, other users can make new wallets and deploy smart contracts on this protocol.

3.1 The Spiderchain

Botanix introduces the Spiderchain, a new primitive for second-layer blockchains. The Spiderchain is a series of successive multisigs between Botanix *Orchestrators*. The security is achieved through the decentralization of these multisig wallets. This series of successive multisigs effectively creates a network that safeguards the Bitcoin of the Botanix chain. This moving chain of multisigs can be seen as a form of collateral that is stuck in this decentralized multisig network; hence, the name Spiderchain.
The Spiderchain effectively separates Bitcoin "the asset" and Bitcoin "the blockchain". By securing the Bitcoin present on Botanix in a decentralized chain of multisigs, it separates Bitcoin from the EVM. This allows for a transition from Bitcoin's UTXO model to an account model used in the EVM.

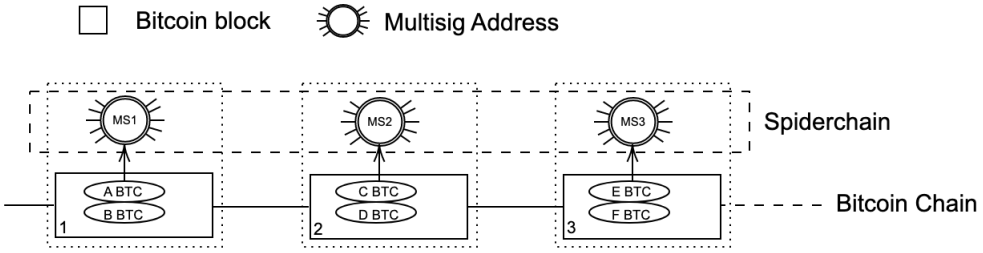
Figure 1 shows a visual of the Spiderchain. Every Bitcoin block creates a new multisig between different random *Orchestrators*.

Since the security depends on incentives and the number of *Orchestrators*, all the *Orchestrators* have to put in a stake before being able to participate. This stake will be used as collateral in case of malicious behavior. The security of the Spiderchain then follows the security models seen in Proof of Stake. As long as the number of adversarial collaborating actors is overwhelmed by the other *Orchestrators*, the security is mathematically guaranteed. There are different tradeoffs to be made in terms of the size of the multisig (in the extreme case, one massive multisig like Nomic [10]) and the required stake. We discuss these tradeoffs in sections 4 and 4.1.

3.2 Orchestrator selection

The Spiderchain will follow a randomized block selection method which will be referred to as the VRF (verifiable random function). The fact that the Spiderchain runs on Bitcoin will be leveraged. We make a distinction between the *Orchestrator* selection in the slots

Figure 1: Graphic depiction of the Spiderchain.



between the Bitcoin blocks and the *Orchestrator* selection for the Bitcoin blocks.
First, the next Bitcoin block *Orchestrators* (meaning the block aligned with the Bitcoin block), will be selected from the block hash. If the number of active *Orchestrators* is N and the block hash is A then the next *Orchestrator* will be $A \bmod(N)$. A delay of at least six blocks must be installed in order to account for possible Bitcoin mining forks. A certain block hash then defines the next *Orchestrator* in six blocks.

Once the *Orchestrators* for the next Bitcoin blocks and multisigs (these define the 'epochs') are selected, every node will calculate the block proposers for the slots in between the epochs. These will be generated from the same block hash as follows: The first slot after the Bitcoin block is calculated by taking the SHA256 hash of the block hash. If the number of active *Orchestrators* is N and the new hash is A then the next *Orchestrator* for this slot will be $A \bmod(N)$. The next slot selection follows exactly the same process etc etc.

3.3 Botanix Blockchain

Botanix operation

The Botanix blockchain operation in steady state has three main parts. First it checks for incoming parent chain transactions (from users to the *Orchestrator*) on the Bitcoin parent chain (the peg-in process). These will have to be lifted up into the Botanix network. Then it will do the necessary state transitions to create a new block. Thirdly to end this cycle, a new set of UTXO's will be created for the unlifting from the Spiderchain back to the parent chain (peg-out process).

1. Check for incoming UTXO's to the Botanix *Orchestrators*. Handle these UTXO's with the peg-in.

2. Run the Botanix consensus and state progression. This part can be compared to the Ethereum block progression.

3. Check for Peg-outs. Handle Peg-outs according to the Peg-out operation.

Note that since the speed of the Bitcoin blockchain and the Botanix chain is different, during most of the blocks, items 1 and 3 will simply be updating the 'mempool' of UTXOs. Bitcoin runs at around 10 minutes per block, while Botanix will run at a faster speed of around 2-3 seconds per block. As in Proof of Stake, the blocks are built by a randomly designated *Orchestrator O*. In between the Bitcoin blocks, these will be EVM blocks. Upon the arrival of a Bitcoin block, the *Orchestrator O* will complete the Botanix operation as described above. This block acts as a 'checkpoint', providing finality for the EVM chain.

3.4 The two-way peg

The currency, synthetic BTC, used on the Botanix blockchain represents Bitcoin and is 1-1 pegged. This means every Bitcoin can be exchanged for the same amount of synthetic BTC on Botanix and every synthetic BTC can be redeemed for Bitcoin on the parent chain. The total Bitcoin locked in the Botanix network of multisigs then equals to the total synthetic BTC present on the EVM chain.
Probably the most important part of any sidechain is how to secure the assets on the parent chain. We will explain here the decentralized protocol of the peg-in and how funds are secured.

The peg-in process

The peg-in process consists of four parts:

1. Incoming UTXO. The current (chosen by the PoS) *Orchestrator O* creates a current multisig address valid for the next Bitcoin block. Alice sends Bitcoin to this multisig address.

2. The *Orchestrator node* O runs the Botanix protocol, includes Alice's UTXO in the opening UTXOs.

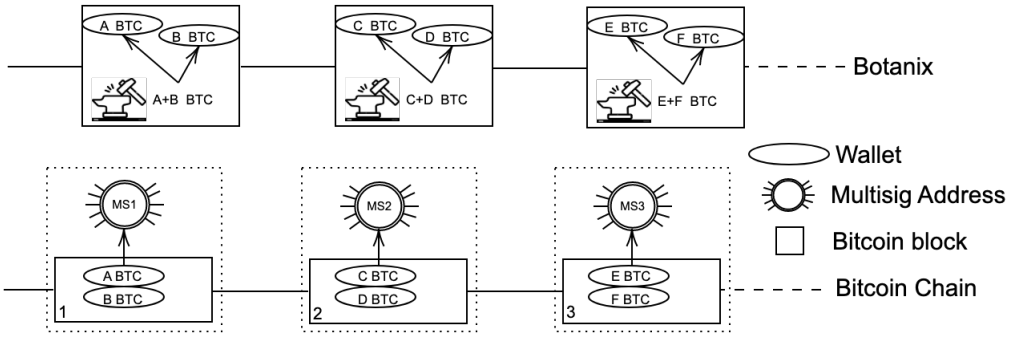
3. After transaction confirmation of Alice's transaction to the Multisig in the Spiderchain, *Orchestrator node* O uses this to mint new synthetic BTC on the Botanix chain.

4. *Orchestrator node* O moves the newly minted synthetic BTC to Alice's synthetic BTC address.

After the peg-in process, the on-chain funds remain secured in multisig chain between the different *Orchestrator nodes* . Botanix uses an account model (in comparison to Bitcoins UTXO model) and any synthetic BTC coins can therefore move freely on the Botanix chain.

Note that the total amount of Bitcoin in the multisigs of the *Orchestrator nodes* equals the total amount of synthetic BTC. This is by design.
Figure 2 shows a visual of the peg-in process. Every Bitcoin block creates a new multisig between *Orchestrators*. In the first block a new multisigaddress named MS-1 is created. This can then act as collateral for the minting of synthetic BTC. Here Alice and Bob send respectively A and B Bitcoin into the Spiderchain which results in the minting of A+B synthetic BTC. The bitcoin transaction fees of the peg-in transactions are paid by the user pegging into Botanix.

Figure 2: Example of a peg-in with multiple *Orchestrator nodes*.



The peg-out process

The peg-out process is similar to the peg-in process in the opposite sequence:

1. Incoming Tx. Alice sends synthetic BTC for a value of A to the address of an *Orchestrator node* O on the Botanix blockchain.

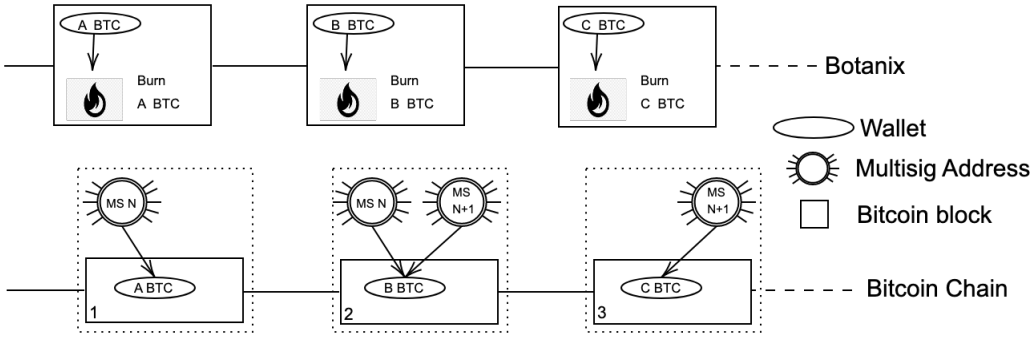
2. The *Orchestrator node* O runs the Botanix protocol, destroys A worth of synthetic BTC.

3. *Orchestrator node* O creates a new UTXO of all outgoing transfers, which includes BTC for a value A. The operation is approved by all multisig signers therefore effectively burning the BTC from the Spiderchain.

4. The multisig address sends the BTC to Alice's BTC address. Honest operation is ensured by consensus.

Botanix will operate on a LIFO basis, meaning that the youngest Bitcoin in the Spiderchain (effectively the oldest multisig) will first be used to send bitcoin back to the parent chain. It can therefore happen that more Bitcoin is pegged out than available on the youngest multisig. Therefore it is possible that the peg-out is split over multiple multisig addresses of the Spiderchain.

Figure 3: Example of a peg-out with multiple *Orchestrator nodes*. The Alice send Bitcoin with value A to an *Orchestrator node*. The peg-out process is started and synthetic BTC is burned. This process enables the oldest multisig address (FIFO basis) to peg-out Bitcoin from MS-N and send this to the Bitcoin address of Alice.



3.5 LIFO inventory

When completing a peg out, there are different ways possible to choose which UTXOs to take. These different options share similarities with inventory management. There is LIFO (Last In First Out) and FIFO (First In First Out) and various hybrid solutions.
Each of the three have benefits and cons. FIFO would be optimal to ensure liveness among the orchestrators and keeping the 'coins' fresh in the sense that oldest UTXOs are spent first. On the other hand, since the coins are refreshed the fastest, any potential malicious adversary will have to wait a certain amount before the coins are turned around and the backwards security of the spiderchain is lost (see more in section 4), therefore FIFO is the

least secure but ensures liveness and has lower tx fees because of the constantly updating utxo pool.
LIFO on the other hand will ensure the oldest coins are secured by the oldest orchestrators, therefore giving a malicious adversary no chance to gain control of these older coins. This does go in pair with higher tx fees as older orchestrators will have to be replaced in their respective multisigs if they go offline. Therefore LIFO is the most secure but has the highest Tx fees.
Botanix chooses LIFO management because of the higher security guarantees.

3.6 Orchestrators: Entrance, exit and erratic behavior

The Spiderchain is an open and permission-less protocol. Here we will describe the process for new *Orchestrators* to enter and exit the Spiderchain. New *Orchestrators* will have to put collateral in a stake and run a full node. Once fully included in the process, they will earn synthetic BTC rewards as defined in the section 4.5 Block subsidy.

Entrance into the Spiderchain To participate in the multisigs of the Spiderchain, a potential *Orchestrator* will signal a participation desire to the designated block *Orchestrator*. As part of his protocol operation, the current block *Orchestrator* will create a new Spiderchain multisig (similar to a normal multisig of the Spiderchain using randomly selected signers) in which a stake will have to be transferred. This multisig will happen in parallel with the Spiderchain multisig creation of a certain Bitcoin block. The stake will act as the stake for the Spiderchain and the Botanix Proof of Stake consensus. After six confirmations on Bitcoin, this staking commitment will announce a new *Orchestrator node*. From then onwards, the *Orchestrator* acts as a full participating node. His participation can be recognized by the Bitcoin block number of the stake.

Exit out of the Spiderchain An *Orchestrator* will signal to the current Block Orchestrator the desire to exit by signing an exit message. From then onwards the exiting *Orchestrator* will no longer participate in the Spiderchain and the exit process will start. Once started, the process continues until the end. The exit process has 3 steps:

1. An Orchestrator signals the desire to exit.
2. All multisigs in which the Orchestrator participates will be replaced by a new random Orchestrator
3. Once all participating multisigs have been replaced, the stake is returned to the Orchestrator.

All the participations in the different Spiderchain multisigs will have to be replaced. In each of the multisigs (see Figure 1) in which the *Orchestrator* participates, all *Orchestrators* will stay the same minus one. A new random *Orchestrator* will join instead. This means

new multisigs are created with the old participants (N-1) plus a new *Orchestrator*. The new *Orchestrator* of the multisig will be the latest one to have joined the Spiderchain (see above entrance into the Spiderchain). The next multisig to be replaced will be the second to last *Orchestrator* to join etc until all multisigs are replaced. The transaction costs of the new multisig creations are considered an exit fee and will be paid from the stake.
As the last step, once the exiting *Orchestrator* is removed from all Spiderchain multisigs, the stake will be returned to the exiting Orchestrator. The exit process is then complete.

Erratic behavior of an Orchestrator When an *Orchestrator* acts against expectations, either on purpose trying to mislead the consensus or by accident, the *Orchestrator* faces potential slashing of its stake. There are four types of uncommon behavior:

1. **Inactivity**. This can occur due to hardware malfunctioning and will result in a slow inactivity leak of the stake.

2. **Incorrect Block building** An Orchestrator could propose a block that is incorrect, or could propose multiple conflicting blocks.

3. **Incorrect signing** of multisigs in the Spiderchain. Either signing a wrong peg-out transaction or a double spend.

4. **Incorrect validation**

Since the concept of the Spiderchain requires the liveness of its Orchestrators (if not, the Spiderchain runs the risk of losing 2/3rd voting majority of the multisigs), a non responsive Orchestrator is a risk. Therefore, inactive Orchestrators will no longer receive block rewards, and after one week of inactivity will slowly be removed from the multisigs per the process described above.
Items 2-4 are considered intentional and are considered slashable offenses.

4 Security

4.1 The size of multisig and stake tradeoffs

The funds locked in the Spiderchain are secured in two different ways. One is security by design, the other security by incentives. By design the funds on the Bitcoin parent chain are locked inside the multisig Spiderchain. A malicious *Orchestrator node* can not access any of the Bitcoin that is present in his account without approval of the others in his multisig. The second is a stake that exists for every *Orchestrator node* that ensures correct operation. In order to participate in the network, *Orchestrator nodes* are required to commit collateral in a stake with the other *Orchestrator nodes*.

Multisig size There is a tradeoff on the size of multisigs. One could imagine one single multisig of 1000 participants [10]. The signing of these 1000 signatures will take a non-trivial amount of time, and possible coordination issues could arise. Moreover, if malicious actors gain control of a 2/3rd majority, they immediately have access to the full amount of capital locked in the Spiderchain. By splitting the collateral into multiple smaller multisigs, the capital at risk is lowered. However, if the multisig size is too small security to protect against malicious adversaries can be lost (see section 4 below) and accidental crashes or key losses can lead to lost Bitcoin.

Stake collateral Since the security depends on the number of participants, an attack vector arises where a single party could run multiple *Orchestrator nodes* while actually being a single entity. This is called a Sybil attack. Similar to the design of blockchains, there has to be a cost associated with running an Orchestrator node in order to avoid an attack. Therefore, *Orchestrator nodes* will have to put in collateral in a stake in order to participate. This puts a real cost towards running a multiple of node. Going offline, acting maliciously or disappearing will result in a loss of funds.

Stake size. A tradeoff exists between the stake size and the number of *Orchestrator nodes*. If the stake size chosen is too big, entities are less inclined to run a node therefore reducing the decentralization. If the stake size is picked too low, the cost for a malicious entity to produce a Sybil attack might be too low.

Liveness Liveness in the case of Botanix can be seen as two different discussions. There is the importance of liveness on the Botanix chain and liveness as participant of the multisigs (while in reality these will be the same). For the Botanix chain, liveness will follow the Proof of Stake implementation. Since the bitcoin is locked into multisigs between different participants, it is important that the participants stay active. Therefore when a participant in a multisig is found to be unresponsive, a new multisig of the same participants (minus the unresponsive participant but including the current Orchestrator)

will be created.

4.2 Forward security of the spiderchain

Forward security is a crucial property of cryptographic systems that protects against the compromise of secret keys. In the case of Botanix, forward security means that even if an attacker gains 2/3rd majority control of the stake, they will not have ownership of the majority of the keys from all the previous multisigs. Instead, the attacker will only have majority ownership of the new multisigs that are generated in the future. This ensures that the security of previous multisigs is not compromised, and the protocol can take appropriate actions to mitigate the attack. By design of the spiderchain, Botanix achieves forward security and the protocol can provide a higher level of security and protect against potential attacks on the system.

4.3 Security analysis

The bitcoin in the Spiderchain is locked into multisigs. There are four variables that result in the security level of Botanix: Size of the multisig, the stake provided by the *Orchestrators*, the total number of *Orchestrators* and the total Bitcoin locked in the Spiderchain. Out of these four, two can be varied: the size of the multisig and the stake required. As discussed, tradeoffs exist for both.
Since the *Orchestrator node* has Bitcoin funds locked up within his wallet address, he can collaborate with other *Orchestrator nodes* to get access to this multisig. The problem he faces is knowing who the other *Orchestrator nodes* are in his multisig. Since they have no control over who will be in their multisig, the probability of this happening becomes lower the more participants in the network.
Let's give a more practical example. Let's take a multisig of 64 participants with a 2/3rd majority. This requires 43 signatures. With 1000 *Orchestrator nodes* running the Botanix network, 63 other random participants are chosen to open a multisig. This is a statistical combination: Choose 63 out of 1000 which gives more than 2^{332} possibilities:

$$Possibilities = \binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{1000!}{63!(1000-63)!} \approx 2^{332} \tag{1}$$

In general, this setup where Orchestrators are randomly chosen to be part of a multisig follows a hypergeometric distribution.
Let Θ be the number of *Orchestrators* of which μ are malicious ($\mu<\Theta$), and let α be the multisig size of which a majority η is needed ($\eta<\alpha$), then the probability of any random newly created multisig to be in hands of the malicious adversary is:

$$Probability = \sum_{x=\eta}^{\alpha} \frac{\binom{\mu}{x} * \binom{\Theta-\mu}{\alpha-x}}{\binom{\Theta}{\alpha}} \tag{2}$$

This distribution ensures that any malicious adversary needs to have 2/3rd of the stake in order to have a sufficient chance of having control of a single multisig.

As a more real life example, let's say a malicious adversary tries a sybil attack and has succeeded to gain control of 33% of the Botanix stake out of a total of 1000 *Orchestrator nodes*. From then onwards, out of all the possible multisigs possibly created, the probability for an adversary to have majority control over a single multisig is

$$Probability = \sum_{x=43}^{64} \frac{\binom{330}{x} * \binom{670}{64-x}}{\binom{1000}{64}} = 7.45 * 10^{-9} \tag{3}$$

Or in other words, the adversary has majority control of around 7.45 out of a billion multisigs. To put this in perspective, there are currently less than one million Bitcoin blocks generated since genesis. So in this example the malicious adversary controls 33% of the stake but has virtually no majority control over a single multisig. Note that the adversary doesn't actually have control, he has only broken forward security.

4.4 Sybil resistance

Sybil resistance is a property of a distributed system or network that makes it difficult or expensive for an attacker to create multiple fake identities in order to manipulate the system or disrupt its operation. In the case of Botanix, we have to look at the individual incentives for every node runner to ensure there is no incentive to collaborate.
An individual party is incentivized to detect malicious action as that party will be rewarded the slashing reward. This is a crucial long term incentive mechanism for honest Orchestrators to detect dishonest parties and get rewarded by keeping the network secure.

On the other hand, a random signer of one of the multisigs in the spiderchain has also an incentive to collaborate with the other signers of that specific multisig, risk getting its stake slashed and steal the bitcoin on that multisig. Since all parties in a multisig know who the other parties are, this allows for any party to maliciously send a signing request (outside of the Botanix protocol) to all other parties. For example, the adversary can send a signing request for a transaction that steals all the bitcoin in a single multisig and divide

it equally among all participants. All the participants of course see this signing request and now have the choice to collaborate or report (read broadcast onchain) this malicious signing request.

Adversarial collaboration between parties will be avoided as long as the sum of the benefits of reporting malicious behavior (slashing rewards) and the costs for erratic behavior are bigger than the potential benefit of adversarial collaboration. A certain party will not collaborate with a 2/3rd majority but instead report this erratic behavior and receive the slashing reward as long as

$$Slashing \quad reward > Adversarial \quad collaborating \quad award \tag{4}$$

The slashing reward is the sum of all the stakes of the malicious actors. We know an actor is malicious if he signs a malicious transaction. Define x as the bitcoin secured in a certain multisig, n the number of participants in a multisig (= the size of the multisig), and s the stake size. The multisig needs a 2/3rd majority. The adversarial collaboration award and slashing reward are then calculated as follows:

$$Adversarial \quad collaboration \quad award = \frac{x}{n * \frac{2}{3}} - s \tag{5}$$

$$Slashing \quad reward = (n * \frac{2}{3} - 1) * s \tag{6}$$

If we expand from this, and using equation 4 a single party will choose to go for reporting erratic behavior and receive the slashing reward as long as:

$$(n * \frac{2}{3} - 1) * s > \frac{x}{n * \frac{2}{3}} - s \tag{7}$$

$$n * \frac{2}{3} * s - s > \frac{x}{n * \frac{2}{3}} - s \tag{8}$$

$$(n * \frac{2}{3})^2 * s > x \tag{9}$$

A malicious party will be indifferent when the above equation is equal. The award and incentive not to collaborate and instead report malicious behavior to receive the staking award goes up quadratically with the number of multisig participants.
Filling this with a specific example, let's assume there is 50 BTC locked ($x = 50$) on a certain multisig of 100 participants ($n = 100$), and the stake size is 3 BTC ($s = 3$). In this case, using equation 9, the decision for one of the 67 collaborators to not join an adversarial collaboration and instead report that a malicious party wants to steal the bitcoin to receive the slashing award, looks like this:

$$(100 * \frac{2}{3})^2 * 3 > x = 50 \tag{10}$$

$$13333 > 50 \tag{11}$$

As long as the amount of bitcoin locked in a certain multisig is less than 13333 BTC, then any participant of the multisig will have an incentive not to collaborate and report malicious behavior.

The reason we look at individual multisigs, is because once an adversary wants to collaborate on multiple multisigs, the slashing award and number of collaborators very quickly increases. Adverse actions for X different multisigs will have a slashing award of

$$X * \#multisig \quad participants * \frac{2}{3} * stake \tag{12}$$

In the previous section we analyzed the probability distribution of the participants in each multisig. Therefore an adversary acting as multiple nodes will have a low probability of being multiple times in the same one and in the minimal probability it happens, the adversary will still have little additional advantage to collaborate as others in the multisig will have a big incentive to detect the behavior and receive the slashing award.

4.5 Block subsidy

In Bitcoin the total reward for the miners to solve the mathematical problem consists of the block reward (halving every 4 years) and the transaction fees. One of the benefits of Proof-of-Work is the fair distribution during initial coin offering while it also offers a drift towards decentralization over time. Energy in the real worlds needs to be purchased and therefore it is a leaking open system where the owners are incentivized to spend to secure the network (in comparison to centralization effects of Proof of Stake). This is however no longer valid in Botanix as Botanix is pegged 1-1 with Bitcoin. It has therefore no or limited impact on Bitcoin's centralization. By owning 1 BTC in cold storage, you will always have exactly 1/21 millionth of all Bitcoin ever to exist.

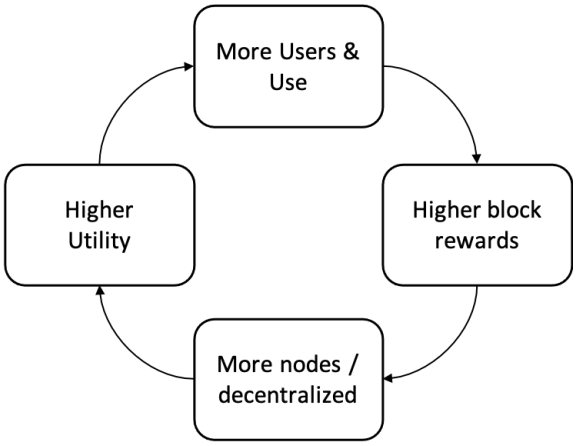
The block reward of Botanix will exist of 3 different items:

1. Base transaction fee
2. Priority transaction fee
3. Downlifting fee when leaving the Botanix network to Bitcoin (UTXO peg-out set)

Since there is be no absolute base block reward possible (because of the 1-1 peg), the situation could arise where no transaction nor peg-outs take place. In that case, the total block reward is 0. There is however still an incentive for entities to run a full Botanix node so they can keep custody and control of their own Bitcoin. Moreover, since the value of Botanix (similar case to Ethereum) comes from it's utility offered, there will be a positive

feedback loop where utility drives more users which in return increases the reward fees which draw in more Botanix node runners which decentralized the network and drives more utility (see figure 4).

Figure 4: The positive decentralization loop for Botanix.



4.6 Bootstrapping

During the bootstrapping phase, the network can be vulnerable to owners with a big amount of Bitcoin. To avoid silent malicious majority attacks, the bootstrapping will happen in 5 phases:

1. Botanix as sole orchestrator
2. Botanix staking pool
3. Permissioned staking pools
4. Permissioned
5. Permissionless

To begin, Botanix will start with a federation. Fifteen independently chosen functionaries will control the first multisig. This puts the security level aligned with (or close to) any other Layer 2 side chains and rollups.
From there, Botanix will form a staking pool where people will be able to stake bitcoin and earn the PoS block subsidy rewards discussed in section 4.5. This will increase the initial stake on Botanix. From there other staking pools, like exchanges and other established

companies will be permissioned to join the consensus. After staking pools, specific individual participants (think whales) will be able to join. And as a final step, with sufficient staking sizes and visibility, staking will be opened to anyone willing to join. From here onwards the protocol is fully permission-less and decentralized.
See Figure 5 for an overview of the different phases.

4.7 Attack review

Sybil attack on the Botanix EVM chain

A Sybil attack, also called a 51% attack, is a threat where one person tries to take over the network. Blockchains use consensus algorithms like PoW or PoS to protect themselves against this attack. Fully removing the threat is not possible, but the idea is to make the attack as improbable or costly as possible.
Since Botanix needs a separate consensus model (malicious Botanix nodes can steal synthetic BTC, not Bitcoin), the possibility exists for malicious actors to attack the network. Here we look at how such an attack could look like and the results of this attack.
As with the proof of stake model, any malicious party could always propose bad blocks. This will result in a slashing of its (Bitcoin) stake. If multiple malicious parties exist, and they end up owning more than 51% of the stake, then they successfully can propose a new Botanix chain that is valid. However the other 49 % will be aware of the attack, and can slash the Bitcoin of the malicious actors. These 49% will then roll out the new chain and own 100% of that stake. This type of attack does therefore not make any sense as there will be very few benefits achieved. The Bitcoin is still locked in the Spiderchain.

Sybil attack on the Spiderchain

Here we look at an adversary trying to steal the bitcoin that is being locked inside the spiderchain. In section 4 we looked at the amount of different permutations possible for a different amount of Botanix node runners. This showed that any adversary will need a 2/3rd majority of the stake in order to be statistically in a majority in specific multisigs. In section 4.4 we looked at the potential for multiple independent adversaries to collaborate and showed that the incentive to be honest is bigger than the incentive to adversarially collaborate. As a result, any adversary will have to be considered a single party. Lastly, in section 4.2 we showed that Botanix is backwards secure and upon breaking the 2/3rd majority, the adversary has only broken forward security: the new multisigs generated in the spiderchain are from here onwards insecure. This ensures that any attacker will need to stay hidden for a long period of time with a 2/3rd staking majority.

Attacking a fully established Botanix is in that sense similar to the stage Bitcoin mining has found itself in over the latest years. Any possible adversary on the Bitcoin miners will attract so much attention in the public space (by harnessing and taking up all new mining

equipment for a certain amount of time), that it will be impossible to stay hidden. After a bootstrapping period and after sufficient size of the protocol has been reached, the same extrapolation can be made for Botanix. An adversary would need to run a big amount of different nodes with each a stake (therefore risking a big total stake that can be slashed). At the same time this would mean the possibility for attracting a lot of public attention on itself. And if exposed, the adversary loses its whole stake. Since Botanix will be more vulnerable to hidden Sybil attacks in the initial stages, the bootstrapping phase will start in a centralized way (see section 4.6).

Long range attack

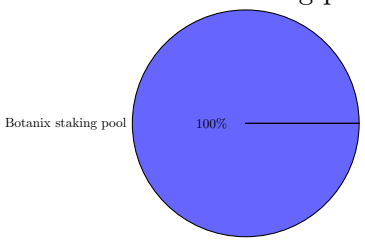
The long range attack is specific to Proof of Stake type consensus algorithms. It involves an adversary secretly creating their own branch of chain, indistinguishable of the normal chain. In the alternative chain the adversary has removed their deposit and are therefore unable to get slashed. The solution is introducing intermediate checkpoints and a timelock longer than these checkpoints. Since Botanix has regular posts on the Bitcoin blockchain, these act as the checkpoints therefore removing the possibility for long range attacks.

Hostage attack

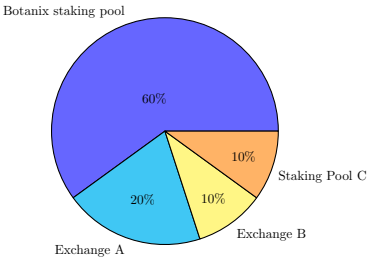
With a 1/3rd majority, any adversary can take the bitcoin in the spiderchain hostage. This means that the adversary can decide no longer to cooperate and decline to sign any peg-out operations. The bitcoin will then remain locked inside the multisigs. See section 3.6 for erratic behavior of Orchestrators. In case of non-cooperation the Orchestrator will slowly over time see its stake reduced due to the inactivity leak.

Figure 5: An overview of the phased approach to bootstrapping the staking decentralization.

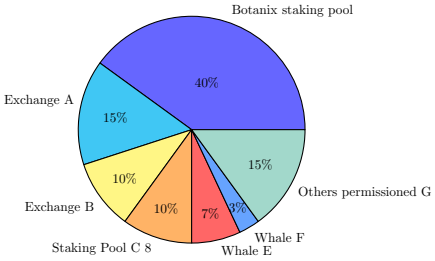
Phase 2: Botanix staking pool



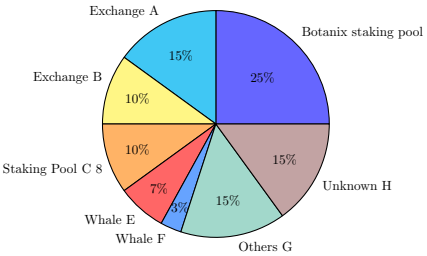
Phase 3: With Permissioned staking pools



Phase 4: Overall permissioned staking



Phase 5: Permissionless



5 Security Inheritance

The security of Botanix depends on that of Bitcoin, particularly the security features provided by its proof of work (PoW) system. If Bitcoin's security were to be compromised, it would also have a negative impact on the security of Botanix. Therefore, Botanix relies on the security benefits of Bitcoin's PoW system to ensure the safety of its own network. More specifically, three risks in any Proof of Stake system that are mitigated by leveraging Bitcoin:

1. Centralization
2. Randomized Validator Selection
3. Finality

Centralization. "The security of a new proof of stake (PoS) system at launch is closely tied to its initial coin offering (ICO). Bitcoin had the most equitable initial distribution of all cryptocurrencies, and this has contributed to its decentralization. Additionally, PoS can lead to further centralization, as the probability of validating a block is proportional to the amount of stake that a validator holds. This means that those with more stake (e.g. more cryptocurrency) have a higher chance of validating blocks and earning rewards, which could lead to the concentration of power among a small number of wealthy individuals or organizations. Botanix inherits the decentralization trend of Bitcoin's Proof of Work and its fair launch.

Randomization. In a proof of stake (PoS) system, validators are typically selected to create new blocks in a randomized manner, with the probability of selection being proportional to the amount of stake that the validator holds. This randomization process is intended to ensure that the system is fair and decentralized, as it allows anyone with a stake in the network to have a chance of being selected as a validator. Randomization is however a difficult problem to solve and the randomization process could be manipulated or gamed in some way, either through collusion or by an individual or organization with a large stake trying to increase their chances of being selected as a validator. Proof of Work solves this by spending energy and solving the difficulty problem. The process of finding a hash is essentially a random one, as miners must try different combinations of inputs (i.e. "nonces") until they find a solution that meets the required criteria. The miner solving the current block in Bitcoin's Proof of Work first is a verifiable random event. A miner finding the solution does have the opportunity to withhold its result and yielding the block reward. Since the benefit (the Bitcoin block reward) of withholding a block is negligible to the edge the miner gains in Orchestrator selection, the Bitcoin block hash production is verifiable random for the purpose of Orchestrator selection. Botanix leverages the randomization from Bitcoin's Proof of Work to ensure a fair Orchestrator selection.

Finality. In a proof of work (PoW) system, finality is typically achieved through the use of confirmations, which refer to the number of blocks that have been added to the chain after a particular block. The more confirmations a block has, the more secure it is considered to be. If in PoS validators are selected to build a block, they have an opportunity to create a fork (one which still has their stake, and another where they withdraw their stake). The potential for slashing and implementing a lock period for staking and solves this type of problem. By being in constant interaction with the Bitcoin blockchain, Botanix leverages the finality of Bitcoin's Proof of Work to achieve finality. The Bitcoin block provides the truth.

Summary. Botanix benefits from the security features of Bitcoin's proof of work (PoW) system and uses these to mitigate the potential vulnerabilities of proof of stake (PoS) consensus algorithms. If Bitcoin were to be compromised, it would have a knock-on effect on the security of Botanix, as it relies on the decentralization, randomization, and finality provided by Bitcoin's PoW system. Without these security benefits, the overall security of Botanix would be reduced.

6 Ethereum equivalence

Botanix runs a full Ethereum Virtual Machine (EVM) execution client and is from a developer almost equivalent to the Ethereum network itself, as it is able to execute all of the same smart contracts and decentralized applications (DApps) as Ethereum. It does not require to generate any validity proofs that would limit its performance as it gains its security from the Spiderchain. The Botanix EVM is the runtime environment that powers the Ethereum network and allows it to execute smart contracts written in Solidity and other programming languages. By running a full EVM client, Botanix is able to support all of the same functionality as Ethereum.

While Botanix is equivalent to Ethereum in terms of functionality, it is still a separate and independent network with its own unique characteristics and features. For example, it has a different PoS consensus algorithm, leverages Bitcoins decentralization and economic structure.

7 Hardware requirements

In this section we take a deeper look at the hardware requirements expected to run a full *Orchestrator node*. Since Bitcoin and the Lightning Network can run on a Raspberry Pi and the Spiderchain does not require intensively more complex computations, the Spiderchain primitive is expected to be able to run on almost any hardware. The Botanix EVM however requires running a full EVM execution and consensus layer. Since the launch of

Ethereum there have been improvements made so that it is expected Botanix can be run on a higher end home desktop.

8 Future research

8.1 Lightning Network compatibility

There are two possible ways to connect the Lightning Network to Botanix. One way involves an intermediate party to swap Lightning Bitcoin to synthetic BTC. In this case the intermediate party would run an *Orchestrator node* and lightning. The intermediate party would receive Bitcoin on Lightning and return the same amount of synthetic BTC and vice versa. The liquidity would be internally managed by the central party.
Another possibility is an atomic transfer for which the possibilities need further research. The setup could look like the following. Each *Orchestrator node* runs on the parent chain a full Bitcoin node. Besides running Botanix, the *Orchestrator node* can also run lightning. When running both a Botanix node and lightning, it is possible to move Bitcoin from the lightning network (LN) to a Botanix multisig in the Spiderchain and the other way around. This multisig would then operate like a channel factory where a channel can be created between an *Orchestrator node* and the Spiderchain multisig. Moving Bitcoin from the Lightning Network to the Spiderchain multisig would then entail a new peg-in primitive (read a new minting algorithm).
While there are no technological reasons standing in between running lightning and Botanix, this does introduce a lot of new interfaces. Further research has to be conducted to see if it is possible for an *Orchestrator node* to open a multisig channel factory where one party is not an *Orchestrator node* but a lightning node and how the new minting algorithm would work.

9 Conclusion

In conclusion, the future of the crypto infrastructure is still unclear, and different approaches are being explored. Decentralization remains the most important property, and technologies like the Spiderchain primitive offer a promising solution to bring smart contracts to Bitcoin, while preserving its decentralized nature. This is key to unlocking a future of composability, privacy, and security for the Bitcoin ecosystem.

The paper proposed a second layer on top of Bitcoin with full EVM equivalence. We discussed the design rationale for building a second layer EVM on top of Bitcoin, the features of Botanix and the underlying protocol. We introduced the concept of a Spiderchain locking the Bitcoin into a network of Multisigs. The Botanix protocol brings these smart contracts in a second layer solution.

References

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: http://www.bitcoin.org/bitcoin.pdf.

[2] J. Poon, T. Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. January 14, 2016

[3] V. Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014

[4] J. Nick, A. Poelstra, G. Sanders. Liquid: A Bitcoin Sidechain. May 22, 2020

[5] O. Osuntokun, C. Fromknecht, W. Paulino, O. Gugger, J Halseth: Lightning Pool: A Non-Custodial Channel Lease Marketplace. November 2020

[6] L2BEAT research team, https://L2Beat.com. November 2022

[7] J. Light, https://bitcoinrollups.org/. November 2022

[8] T. Del Bonis https://tr3y.io/articles/crypto/bitcoin-zk-rollups.html. March 2022

[9] V. Buterin "What kind of layer 3s make sense?" https://vitalik.ca/general/2022/09/17/layer_3.html. Sept 2022

[10] M. Bell "Proof of Stake Bitcoin Sidechains" https://gist.github.com/mappum/da11e37f4e90891642a52621594d03f6. Dec 2022

[11] Bernardo David and Peter Gazi and Aggelos Kiayias and Alexander Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol, Cryptology ePrint Archive, Paper 2017/573, 2017, https://eprint.iacr.org/2017/573

[12] https://www.web3.university/article/sidechains-vs-layer2s Dec 2022