Introduction

Cryptocurrencies, as they exist today, are walled gardens, which cannot reuse, trigger, or execute transactions with other blockchains. Think of each cryptocurrency as a landlocked nation capable only of trade and transaction within its own borders. Humanity has learned over millennia that open economies are exponentially more conducive to shared growth and prosperity. In the same way, we believe the blockchain ecosystem becomes more useful and more powerful when blockchains are able to work together, instead of competing against or ignoring one another.

Block Collider makes multichain interoperability fast and scalable in an unprecedented fashion. We do this by remaining lean enough to have stable, low-latency transactions but robust enough to incentivize miners and to simplify workflows through unification. Uniquely, Block Collider is able to maintain *true* decentralization. This means avoiding compromises such as centralized oracles and validators to interact across chains. Fundamentally, we will always choose to do things the right way, rather than the easy way.

Motivation

There are more than 1,800 cryptocurrencies in existence today, all with their own unique approaches, differentiators, and claimed benefits. Some chains claim quick block-times as their advantage, some have smart contracts, others are purely a store of value, and so on. While the most useful of these currencies bring functionality with some benefits, they all share the encumbrance of an old constraint: double work.

Consider this scenario: If one seeks to include new functionality from *Chain A* onto another protocol, *Chain B*, then one would have two options—either to build that functionality, often completely from scratch, into the protocol, or to purchase *Chain A* and integrate the two chains. The latter option would not only cost significant time and resources but also force the use of a trusted mechanism. While both of these options lead to the same end result, they are by no means the most effective or efficient routes conceivable. More importantly, the founding principles of cryptocurrencies have always been about optimizing the way problems are approached. In this spirit, Block Collider creates a bridge between chains, completely bypassing the double-work taking place in the industry by opening up functionality from each chain in the network to anyone who builds on the protocol.

If a plumber tries to fix a faucet, they may need only a wrench, but then again they might need everything in the toolbox. In the ideal scenario, professionals should have access to whatever tool will solve the problem best. Block Collider believes that equipping the blockchain industry with the ability to cooperate across protocols is an essential step in our progress.

Implications

The implications of Block Collider's decentralized multichain platform are dramatic and truly exciting:

- **Freedom to execute not only cross-chain, but chain-agnostic transactions and smart contracts.** On Block Collider, people can execute a value transfer transaction in a fraction of the normal time by routing that transaction through the fastest of the bridged chains. With all chains working together, the limitations of operating under just one chain fade away, allowing optimized progress.
- **Cross-chain transactions will be *truly* decentralized**, unlike all other existing cross-chain protocols—no validators, no oracles, no "trusted nodes." Without centralized points of vulnerability, cross-chain transactions can flourish, unhindered by costly and needless risk.
- Blockchain **provides engineers with better building materials.** They can use exotic functionalities from connected chains and previously impossible load-balancing methods when building decentralized applications on Block Collider.

Adding to the excitement, all these features, and more, are available on Block Collider without a single line of code being changed in member protocols.

Use Cases

What do these implications look like in practical use cases? The following are just a few examples of applications and their functionalities that could run using Block Collider.

- **Multi-asset decentralized exchanges (MADEX)**
    - Trade not only token-to-token on a given blockchain, but trade across blockchains.
    - Relentless, anonymous, and unstoppable trading: bandwidth issues, similar to those we saw on Ethereum during the height of CryptoKitties, cannot throttle trades if the flexibility present to use the best chain available at the moment.
    - Trustless decentralization without compromise and without validators that can be manipulated.

- **Meta-contracts**
    - Chain-agnostic contracts allow users to take advantage of whichever chain makes the most sense within a given set of parameters. An example of this advantage can be see in in the implementation of exchange insurance. If a payment chain breaks, insurance contracts can be executed with value from another chain.
    - Guaranteed contracts guarantee that nothing can stop the contract from executing, not even the originating chain. A possible use-case (discussed later) would use encrypted transactions to enable whistleblowing-like events that could be decrypted through a meta-contract if some predetermined action is not taken.

- **Next-gen Dapps**
    - Dapp developers can avoid pitfalls and choose the right chain for any given job.
    - ICOs and crowdsales: New projects could use a Block Collider meta-contract that would accept tokens from any supported chain.
    - Decentralized Ridesharing App: Rider/driver reputation data should be secure (Ethereum), GPS/communication should be fast (Lightning Network), and payments should be friction-free (Block Collider meta-contract).
    - Banking transfers: Transactions should be fast and cheap (Ripple), but use a more powerful chain (Ethereum), to handle complex contracts, as opposed to relying on trusted entities (legal contracts, lawyers, and others) to enforce contracts and transfers.

Data Structure

Multichain vs. Blockchain

At its simplest, a blockchain is a series of timestamped transactions. Originating with the Bitcoin blockchain, these timestamped transactions began in the form of value transfers (sending BTC from person A to person B). These transactions eventually became more complex with the advent of Ethereum, where transactions were in the form of either value transfers or data transfers (calling a function on a smart contract that altered the information being stored on that smart contract). Regardless of what type of transfer, by having a timestamped history of all the transactions, a blockchain can ensure the viability of future transactions (one cannot send 100 BTC if one only has 90 BTC).

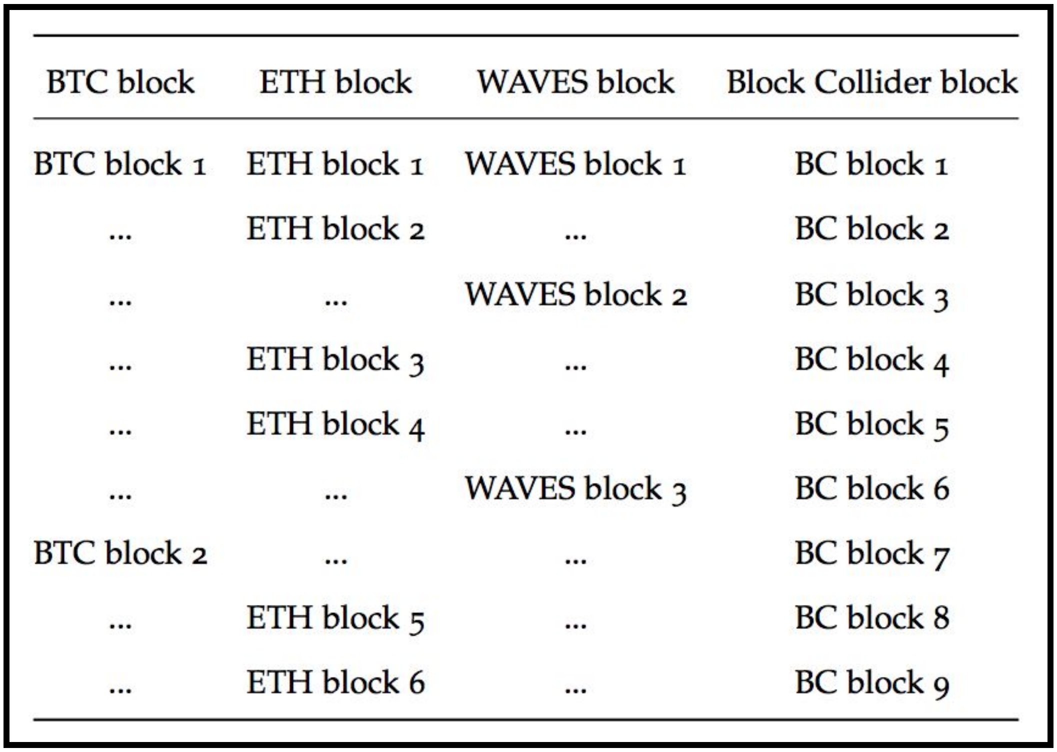
A multichain on the other hand is a series of timestamped blockchains. By knowing the history of blockchains and their underlying transactions, one is now permitted to transact between them with full knowledge of the state of all these blockchains, in a decentralized manner. For instance, in order to effectively collaborate on a group project, all members should have up-to-date information. Similarly, Block Collider can work effectively because it knows the latest blocks from each blockchain. This is the core functionality of Block Collider; maintaining the current state of all supported chains without centralization. Knowing and using the most recently mined block on all member chains ensures the validity of transactions between them.

Weaving Chains

From a continuity standpoint, consider a transaction between BTC to ETH: Both have mined blocks of data that are chained sequentially, with each block using the previous block's header-hash as part of its data. Linking header-hash numbers between blocks is one of the key security functionalities in minable blockchains. If one link in the chain is inaccurate, it is easy to tell as each block relies on the accuracy of data from the previous block. This is the same security measure used by Block Collider, only on a larger scale. Using the most recent block of BTC along with an ETH block from one hour before in a cross-chain transaction could result in unauthorized credits/debits and double-spending. Since most chains have varying block times, transactional accuracy can be accomplished only by having a reliable, up-to-date pulse on each supported chain.

Transaction accuracy on a multichain can be compared to the precision of an orchestra conductor. Each musician has different notes to play at different times, but the conductor keeps track of every instrument, adjusting tempo and volume where necessary. This role creates harmony by weaving together individual instruments as members of a larger whole. If the conductor doesn't know the composition or all of the players' roles, the result is dissonance. This is true of the multichain orchestra—there must be a reliable conductor!

Block Collider fulfills this role by combining the most recent header hash from each of its bridged chains into a *tuple* (an immutable sequence) and updates this "base tuple" as each of the supported chains completes a block. This flexibility allows Block Collider to act as a unifying chain that is faster than the fastest block-time of any of its bridged chains. If BTC has a block time of 9 minutes and 12 seconds and ETH has a block time of 30 seconds, the Collider's base tuple will be updated on average every 28 seconds. This compounds as more blocks are added into the mix. Note the staggered nature in the table below (not to scale) of each of the three sample chains' completed blocks, and how Block Collider acts as the unifying method that keeps track of the most up-to-date chains.



BTC block	ETH block	WAVES block	Block Collider block
BTC block 1	ETH block 1	WAVES block 1	BC block 1
...	ETH block 2	...	BC block 2
...	...	WAVES block 2	BC block 3
...	ETH block 3	...	BC block 4
...	ETH block 4	...	BC block 5
...	...	WAVES block 3	BC block 6
BTC block 2	...	...	BC block 7
...	ETH block 5	...	BC block 8
...	ETH block 6	...	BC block 9

By weaving the most recent blocks together using the base tuple, Block Collider provides a straightforward way to ensure the validity of transactions across all bridged chains.

Block Velocity

Miners on Block Collider will be mining for blocks using combinations of the supported chains. As the number of chains grows, so does the complexity of the computational difficulty of mining the multichain. This has the added benefit of preventing attacks that employ increased mining power on Block Collider. Over time, the number of new blocks created in a given time period will grow. The speed of that growth is the block velocity of Block Collider.

Because Block Collider is a multichain, the block velocity of Block Collider can also be described as, with a little variance for hashing time, the sum of all bridged chains' velocities. Since block intervals (time between blocks created) are the inverse of the block velocity, Block Collider's formula for block intervals is fairly simple. This is a great quality for a minable blockchain; as the velocity increases, the mining difficulty increases and transactions will naturally slow down unless the block difficulty is throttled. Block difficulty (Block Collider's function for naturally throttling mining difficulty based on the supply of mining power) is a function of block interval. The cleanliness of the block-time formula then allows for uncomplicated adjustments to the mining difficulty order to prevent slow-downs and maintain low latency.

Multichain Conflicts

Since Block Collider relies on the blocks of its supported chains, issues native to those chains are inevitable. For example, if there is a disagreement on the validity of the most current blockt, which happens frequently on minable chains, then that issue will carry over to the Collider.

For clarity, when a block disagreement happens on a given chain (when an orphan or an uncle is created) one of two things will happen over time. Either the forked chain will die-off because a majority of miners do not agree that it is the next valid block, or the forked chain will have a majority of miners agreeing on it's validity and it will therefore become the "true" chain. The process varies from chain to chain, but essentially this is how most protocols overcome this issue. This is also what technically happens when a project is hard-forked (i.e., Bitcoin or Bitcoin Cash).

Fortunately hard forks actually turn into an advantage for Block Collider. Since the policies of each member chain directly impact chain resolution, and those policies vary from chain to chain, Block Collider permits all valid blocks (including orphans and uncles) from supported chains onto its base tuple. Simply, uncle and orphans will also get ingested into Block Collider. And when a winner is decided, Block Collider's chain adjusts to that as well, given miners will be receiving blocks from a majority of the child chains. This process creates more blocks and further speeds up block times. It also gives the native chain room to decide the winner on its own terms, as at the time of creation; orphans are not orphans, they are simply options. By including the hard-fork process, not only does Block Collider circumvent the need to keep track of each chain's winning block policies, it also gains block velocity by creating a new Block Collider block.

Proof-of-Distance

There are now a variety of consensus models in the blockchain ecosystem, with Proof-of-Work (PoW) and Proof-of-Stake (PoS) being the most common. Using PoW to build a multichain is not feasible due to the extreme difficulty of finding a nonce that fits the PoW requirements of all the underlying chains. A nonce that fits the requirement for Bitcoin will not necessarily work for Ethereum, and finding one that fits both will take exponentially more compute power. Using PoS to build a multichain is also not feasible given the centralization that would occur using such a model. In addition, due to the nature of PoS, in the event of a chain split, there would have to be a centralized mechanism to choose the correct chain.

Consensus Approach

The mechanism Block Collider uses to weave the bridged chains together is built into the multichain's consensus mode, Proof-of-Distance (PoD). Competitors in the space, as mentioned earlier, use validators or trusted nodes to find the latest block-state for every chain they are bridging. Block Collider takes a different approach, tasking its miners with solving for PoD, a variation of Proof-of-Work which is based on Cosine Distances. Cosine Distances are frequently used in radio and cell networks for eliminating backscatter and establishing efficient communication across disparate data types. Applied to a multichain, PoD involves miners who receive the latest blocks from each bridged-chain. They are tasked with finding a hash that lies between all of the header hashes of that miners have collected from the bridged chains. Consider a color wheel on which specific shades of purple and red are marked. An artist could eyeball the midpoint between those colors, but to know exactly what shade of pink to use, they, you would need to know the exact shades of the original colors. This is what PoD allows for, as it is a mathematical and fully decentralized solution to finding the "intermediary hash" of all bridged chains at any given time. Miners who successfully find the closest intermediary hash, thereby creating the next Block Collider block, are rewarded in NRG, the native currency in Block Collider's multichain (NRG is explained in following paragraph). There is only one next block, making for a hypercompetitive mining process, which will only scale as more bridged chains are included into the protocol.

Token Dynamics

So how does Block Collider actually implement the decentralized multichain? The core technology behind Block Collider's protocol is found in its new Proof-of-Distance mining algorithm, which both creates new blocks and maintains the state of all bridged chains, while utilizing three useful components that will fuel Block Collider's ecosystem.These components include NRG, Emblems, and Marked Tokens.

NRG

Non-Relational Graph (NRG) is the minable currency of the Block Collider multichain. It is the primary fee used for conducting transactions and rewarding miners. NRG functions similarly to "Gas" on Ethereum, however NRG is a separate currency. Having such a currency is necessary to ensure that parties transacting on the multichain pay for the computation required to execute each of their transactions, which is ultimately key to incentivizing miners to keep the multichain alive. There is a fixed supply of NRG (approximately 9.8 billion), which means that Block Collider's reward for mining is naturally reduced over time as the NRG supply is disbursed.

Emblems

Emblems (EMB) are meta-tokens. They will initially represent a basket of other uniquely marked tokens from each of the bridged chains. Those marked tokens are used as keys to access the different functionalities between chains. Similarly to NRG, there is a fixed number of Emblems (300 million). Unlike NRG there is no way to mine Emblems. When owned or leased by a miner, Emblems enable an increase in the size of the blocks they mine, allowing them to fit more transactions into that block, thereby earning more fees per block mined.

The first version of an Emblem Leasing Portal, an interface for renting out Emblems, will be released by Block Collider. This will be a necessary part of the ecosystem, preventing Emblem hoarding and putting these assets to good use. Emblem holders will be able to place orders, requesting ETH in exchange for access to their EMB for a certain lease period (6,12, or 24 months). Once a lease is acquired, the purchaser can either use this lease to associate the underlying EMB with their account or, if they desire a shorter lease time, trade these leased Emblems (L-EMBs) to another party. Once the lease is expired, the EMB will be available for retrieval by the original lessor.

That being said, miners do not need any Emblems to mine on the Collider. An Emblem is a value-add for miners. If blocks are shopping carts where transaction data can be packed like soup cans and milk cartons, Emblems are a way for miners to expand the size of their shopping cart. The more transactions they can add to their block, the more fees they can collect, creating an incentive for miners to own Emblems. Nevertheless, the number of transactions gained based on Emblem ownership diminishes on a logarithmic scale, to combat any incentive for central ownership of Emblems.

Marked Tokens

Marked tokens, which make up the Emblems mentioned earlier, are a crucial part of initiating cross-chain events or transactions with the Block Collider multichain. If any of these marked tokens are added as part of a new block in any of the bridged chains, Block Collider will automatically add that transaction to the Block Collider chain. This can, in turn, trigger other actions across multiple chains using a Block Collider meta-contract. The process that miners go through to find the current state of all chains has been mentioned earlier, but to know which transactions from those bridged chains are relevant and should be added to a Block Collider block (as copying all transactions from all chains is unfeasible) there must be some form of demarcation. This is the purpose of marked tokens; by using unique tokens on each of the bridged chains, miners can trigger cross-chain events. There is also a method for Block Collider miners to add transactions from unmarked token transactions, but these will incur a fee.

Mining

Block Mining & Transaction Mining

Most blockchains have both transactions and proofs listed in their blocks. Block Collider takes a more focused approach by separating block mining from transaction mining, and empowering miners to use their computing power in the way that makes the most relative financial sense. As block mining will naturally add chains, scale, and become more labor-intensive, transaction mining will remain accessible to smaller players.

Transaction mining also uses PoD, however, instead of header hashes from bridged chains, miners are tasked with computing any transaction equations and then finding a nonce that, when combined with the miner's public key into a hash, is a certain edit distance away from the transaction hash. Once found, this transaction will get added to the next block and the miner will be rewarded in NRG. The edit distance away from the transaction hash is important because blocks are capped at the total edit distance variability their block can have. To illustrate, we'll return to the shopping cart with the milk carton analogy mentioned in the Emblems section:

If Alice is are tasked with buying milk for a group breakfast, and she arrives at the grocery store, what is her first move? Alice would look for the largest milk containers. When Alice nearly fills her care, she notices that all the remaining large containers of milk on the shelf are expiring tomorrow. She could add these to her cart, but it might be risky—her group may end up with spoiled milk and that would ruin the whole breakfast. Logically, Alice's next move is to fill her cart with the smaller cartons that have longer shelf-life, a sure thing when it comes to avoiding spoiled milk. Having filled her cart, she leaves the grocery store successful and is welcomed to the breakfast as a hero.

This is essentially the economy created for transaction miners. Remember, there is a limited edit distance variance allowed in each block (which can be compared to the risk of buying spoiled milk). Larger transactions take more effort to mine and have higher rewards (i.e., those larger cartons), but transactions most likely to be included in the block are those with a lower edit distance (the smaller cartons that are definitely not spoiled) because miners will always want to fill their blocks (shopping carts). Transaction miners will optimize for lowering edit distance rather than the number of transactions based on market value. When the transaction edit distances in blocks are capped, miners are incentivized to invest their computing power wherever it makes the most relative financial sense. As blocks get filled, there will always be an active market for both larger transactions with higher edit variability and smaller transactions with lower edit variability. This leaves the playing field open for anyone who wishes to mine transactions on the Collider, as there will always be multiple winners.

Key Takeaways

By splitting the mining of blocks and transactions, Block Collider plays to the strengths of each while avoiding common issues that would arise if they were conjoined. Block mining will always be a more competitive landscape, where the next block is an extremely scarce resource, while transaction mining will be much less competitive because there can be multiple winners. By splitting the economic incentives into two camps, the chance of centralization is significantly reduced. Achieving centralization in both camps requires almost opposite optimization strategies. While acting as a protective layer, this split also allows for unprecedented efficiency gains in the mining market through specialization.

Transactions

Blockchain transactions generally refer to the sending and receiving of cryptocurrency, which is then recorded on that specific blockchain ledger. A transaction on a blockchain refers to an event that alters or appends information to a database. In the case of Bitcoin, a transaction is the act of sending BTC from party A to party B. In Ethereum, a transaction can include changing the name of Crypto Kitty to Sir Nakamoto. Transactions on blockchains can trigger transactions of their own, but only on that blockchain itself. A multichain transaction, on the other hand, refers to a transaction on blockchain A that is triggered by a transaction that occurred on blockchain B.

Recent attempts at creating decentralized marketplaces have been helpful for the progress of the industry, as they have introduced new functionalities for trading. However, their functionality ends at the limit of each blockchain. This limit, or final frontier, is as much a technological challenge as it is a value indicator for greater adoption; if we can bridge the divide in a fully decentralized manner, it will act as a tipping point for mass adoption of the technology in place of centralized services.

Some well-intentioned early initiatives (Token, Swap, ox) exclusively trade ERC-20–based tokens and are therefore subject to the limitations of Ethereum's protocol. This is the crypto equivalent of browsing the Internet using Netscape—or for those who enjoy more accurate technical comparisons, an early but limiting Internet protocol called UUCP. It got the job done and proved the concept at the time, but there was so much that was yet to be discovered. Take Ethereum's block speed, for example. Since a new Ethereum block is formed every 30 seconds, the completion of a trade could take minutes, sometimes longer, especially when the submission of the trade and acceptance of the trade are on consecutive blocks. Trades that take minutes to complete are a far cry from where they should be compared to mature financial markets. The technical limitations are of course dwarfed by the true shortcoming; that a majority of the cryptocurrency market volume is not ERC-20 based (BTC-ETH ratio alone is 3-1 in volume). Those who try to build solutions outside of ERC-20 rely on some form of centralization in their core technology (validators, etc.). It is necessary to mention solutions such as atomic swaps or solutions built on atomic swaps, such as the SparkSwap or the Decred DEX. Atomic swaps do not use "validators" per se, but they do utilize the Lightning Network to execute their hashed time-lock contracts. By virtue of relying on the Lightning Network's trusted nodes to execute contracts, these solutions are ultimately centralized to some degree. As established in previous sections, exchange services built on Block Collider will be able to serve their order books faster than ever before and will have the ability to perform true cross-chain trades, not simple "token swaps," in a truly decentralized way.

Multichain Transaction Basics

It is important to understand how multichain transactions work in Block Collider. A multichain transaction looks very similar to any normal blockchain transaction, with the caveat that there are certain flags within a transaction that indicate which underlying blockchains to use and which transactions to look out for in order to execute the underlying promise, if any.

Once transactions are submitted to Block Collider, miners need to verify and process those transactions, placing them into a block. In order to accomplish this, miners must effectively have access to each transaction that is issued on the network to ensure new transactions are valid. However, it is not feasible to require that each miner know about every transaction on the network at any given time before issuing a block. Imagine instead, a realistic scenario where users issue transactions at a rate of one per second, but it takes the entire network about two seconds to sync all transactions. The network would never be able to issue a block! Instead, Block Collider uses a distributed hash table (DHT) to store these transactions. This means that individual miners only have to store a subset of all pending transactions in their transaction pool while querying other miners for any other pending transactions that are missing to ensure that a given new transaction is valid. As Block Collider miners communicate with their peers, they will routinely update each other on their pending transactions, creating a comprehensive and distributed map of transaction timelines. Using a DHT (assisted by rovers, which will be discussed later) to store transactions greatly decreases the latency between verifying new blocks, and keeps Block Collider's miners moving at optimal levels. Additionally, since Block Collider is a multichain, the DHT stores the current state of not only one chain, but all bridged chains. Maintaining this current state is what allows the execution of transactions using events across multiple chains.

Promises

Promise transactions are another new functionality in the multichain space. The basic premise of this type of transaction is pretty fascinating. Promise transactions offer a way of encrypting and decrypting data on the blockchain using transactions. For example, whistleblower Wendy submits a transaction, TxA, on a specific blockchain, but the data within that transaction is encrypted. This data is "evidence of corruption," but, again, it is encrypted. Wendy has also created a smart contract that will decrypt TxA's data, but if and only if it has not received a specific transaction from Wendy at some preset interval of time. Wendy can now "leak" the secret at any time by simply not doing anything. This also gives her an "insurance policy" in case something were to happen to her. This decrypted data revealed by the smart contract can then be accessed by anyone in the world. Checkmate!

Unfortunately for Wendy, in the current state, her promise transaction must reside within one specific chain, which, as we mentioned previously, means she is subject to that chain's limitations (bandwidth, block times, block size, etc.). Wendy would also have to rely on a third-party to execute her smart contract to decrypt TxA, leaving her vulnerable to centralization. Wendy can decentralize and protect her promise transaction, while serving justice, by deploying a Block Collider meta-contract. This would enable her to place TxA on whichever of the bridged chains she wants! A decentralized, multichain promise transaction is another function that is possible on Block Collider.

Callbacks

The enterprise version of atomic swaps, callbacks are a market-ready technology for conducting cross-chain transactions between blockchains. In application, callbacks are two or more promises that have been chained together to facilitate a cross-chain transaction. Similar to the promises from which callbacks are made, a transaction can be decrypted and even deployed by a separate connected transaction. Callbacks are executed in two stages: setup and fulfillment.

Each action after the setup stage is ensured using collateral, offered by whichever party has the opportunity to defect and walk away. In this way, if one of the participants defects, tries to cheat, or ends the transaction early, the non-defecting party is guaranteed the collateral. An example of a callback is if Bob wants to trade X amount of BTC for Y amount of ETH. This callback transaction would get submitted, posting the promise of Y for X and automatically creating a bonus wallet, which will hold the collateral for the deal. If Alice wants to trade her ETH for Bob's BTC, she can create a response callback transaction, which also creates a collateral wallet. Once the setup is complete, the transaction can be broken up into as many fractions as necessary for both Bob and Alice to be happy with the collateralized amount. This type of incentive-compatible transaction on Block Collider goes a long way to improve confidence in a cross-chain ecosystem.

Looking to the Future

The multichain space is constantly gaining momentum, as the need is increasingly obvious as the industry matures. It is expected that Block Collider will continue to grow and evolve, but it will need to do so in a truly decentralized way. The following are expectations for changes to be made to the software and the direction in which Block Collider intends to progress.

Development Considerations

One of the more obvious improvements is to add or remove chains. Block Collider is designed for the easy addition of new blockchains. The mining load and computational challenge will be minimally impacted, and the difficulty threshold will be adjusted to maintain continuity. The process of how those new chains are to be added will be included in Evolution Mode (discussed below).

There will be planned forks, or critical updates, that occur over the first three years after main net launch. These forks will include bug fixes, compatibility for new blockchains, efficiency improvements, and other related updates. At the end of these forks, (of which there will be no more than six), we will release a voting protocol as the primary way of governing Block Collider multichain moving forward. This voting process is called Evolution Mode and spans a three-month period during which new blockchains can be voted into the Collider and unwanted blockchains can be voted out. *Evolution Mode* will also allow for "architect voting," where Emblem owners can submit (with some personal staking) a project or proposal to Block Collider. This could be a request for funding to develop a new feature or a change to a previous feature.

Evolution Mode serves three purposes. First, it gives Emblem owners a direct relationship with the evolution of the chain. Second, it allows the Collider to adopt new features through a democratic process. Third, it allows Block Collider to create features and organically grow with involvement from the community. By equipping Block Collider with the tools to self-govern, the multichain can remain trustless and truly decentralized.

An important aspect to note relates to incentives to hold onto Emblems. There are three main reasons individuals could potentially hoard Emblems: miners looking to increase their fees earned per block mined, speculation (money-under-the-mattress types), and voting influence. The concepts of diminishing returns on Emblem ownership for block sizes as well as Emblem leasing have already been covered, and both adequately solve the first two hoarding incentives. We don’t anticipate any voting cartels being created, but we are actively exploring voting models in an effort to stay ahead of potential issues.

Vision and Future Direction

Blockchain technology has come a long way since Satoshi Nakamoto first released the Bitcoin white paper in 2008. While there is certainly a degree of frenzy in the industry at the moment, many are seeing and developing practical applications of this technology. Such initiatives will drive the industry to solve problems we have not yet been able to solve. Blockchain may indeed herald a new world where individuals, simply by having access to private information, can be cryptographically assured of their rights and freedoms. This is a worthwhile goal and is the top priority Block Collider.

The industry as we know it, however, is strongly siloed. While current systems grant users freedom within their domain, users are still confined within that system. Many solutions to the multichain problem rely on centralization, which is fundamentally at odds with both the values and advantages of cryptography. By weaving together disparate chains into the Block Collider multichain in a truly decentralized way, we can enable a new level of individual choice without relying on gatekeepers to gain access to those choices. The Block Collider team is dedicated to the cause of promoting freedom through cryptography. In many ways, Block Collider is not a competitor to other cryptocurrencies, but an enabler that validates and empowers all other currencies. A rising tide lifts all boats.