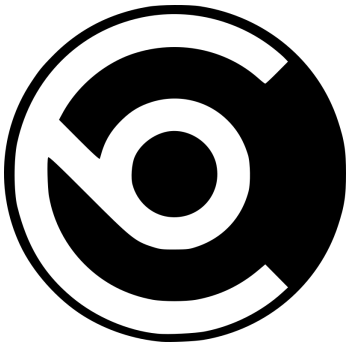
BLOCK COLLIDER WHITEPAPER



BLOCK COLLIDER TEAM

created: February 11, 2017

revised: January 17, 2018

v0.9.9

CONTENTS

"Write programs that do one thing and do it well. Write programs to work together."

— Doug McIlroy, the inventor of Unix pipes[14]

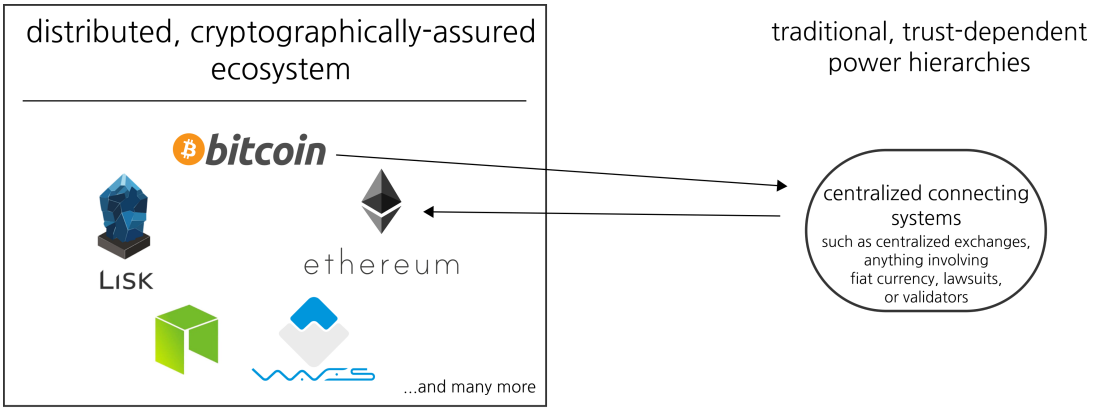
1 INTRODUCTION

The Block Collider multichain is a high-speed distributed ledger built on sets of blocks from other blockchains, integrating those chains together and enabling many cross-chain features. The multichain supports ultra-low latency balance updates with the Financial Information eXchange (FIX) protocol and innovates on reduplication of work and incentives for miner network speed, so that the resulting multichain pushes the frontier of speed and throughput of blockchains. The Block Collider multichain is collaboratively created exclusively by decentralized peer-to-peer miners — with no centralized points of failure, oracles, or validators.

1.1 Motivation

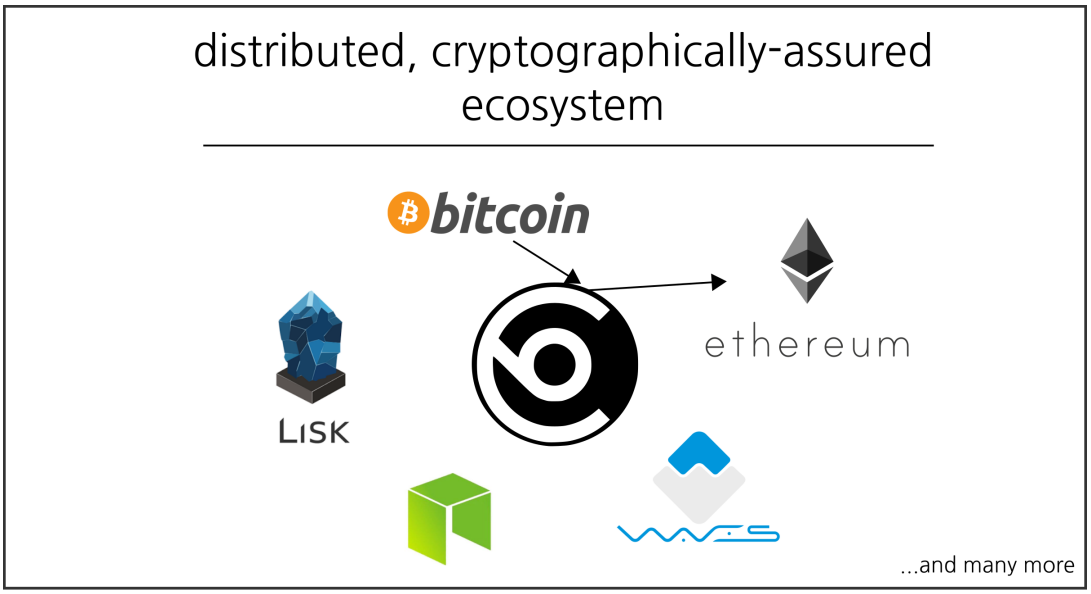
Cryptocurrencies are "walled gardens" which cannot reuse, trigger, or execute transactions with other blockchains. If Alice wants to execute Bob's smart contract, she can only send cryptocurrency from the blockchain on which Bob deployed the smart contract. This lack of cooperation stifles innovation and drastically inhibits practical use.

Block times and fees make many blockchains ill-suited for heavy transaction volumes or trading. Sidechains erected to alleviate the pressure centralize the network and are in the hands of a few mining pools or startups, isolated from the paradigm advances of decentralized design, and at the mercy of power structures which require unwarranted trust.



Bridging chains with a multichain is like building roads between buildings. Hypothetically, one could build a building that has everything, but in practice some buildings are built to work in, some are built to live in — as long as citizens want to be in multiple buildings at different points in time, roads are valuable. The crypto community as it exists demonstrates a wide variety of features across blockchains — some chains have quick block times, some chains have expressive smart contracts, some are purely deflationary and an excellent store of value. As long as users need features from more than one blockchain, bridging those chains with a multichain is needed.

This is why Unix design philosophy recommends that each program do one thing well[14], and that the operating system should make connecting those excellent modular pieces simple and efficient (for example, via pipes). The Block Collider multichain enables this philosophy for blockchains by providing the opportunity for interchain communication and cooperation.



1.2 Implications

With the adoption of Block Collider's multichain technology:

- transactions and smart contracts can initiated or executed by smart contracts on other blockchains
- secure transactions can be bridged between blockchains without "witnesses", "trusted nodes", or centralization of any kind
- transactions between chains can be sped up beyond the speed of either bridged chain
- smart contracts can be guaranteed to execute automatically

- distributed application developers can modularly combine exotic features from blockchains across the ecosystem
- distributed application developers can build in the capability to load-balance work between chains

All of these features can occur without code changes to any of the bridged chains — the system is designed to be compatible with the existing ecosystem. Moreover, with its quick block times, and with the drastic deduplication of work that its architecture provides, the Block Collider makes an exceptional platform upon which to build truly decentralized systems.

1.3 Use Cases

Multichain technology is a crucial next step for the crypto ecosystem. The following are a few examples of key use cases which the Block Collider multichain technology enables.

Decentralized Exchanges

Exchanges are currently a primary bottleneck in the crypto industry. Being listed on an exchange is a primary driver of prices for crypto assets, and technical issues for exchanges detrimentally impact the industry as a whole. Block Collider's multichain would allow exchanges between cryptocurrencies to be performed without any central point of failure, which brings the inherent network robustness characteristics of blockchains to bear on this crucial industry function.

Cross-chain Smart Contract Hedges

Protection from hacking is a primary concern for many participants in crypto markets, as security breaches have caused significant loss of capital. Because Block Collider's multichain can trigger an action on one chain when an event is triggered by another, one potential use case is to provide smart contract hedges. That is, when an account on one blockchain (known to be inaccessible to any but the hedge provider) is emptied, an account on another blockchain is credited with the amount lost. Thus, third parties can secure against security risk in a cryptographically ensured manner.

Automatic, Guaranteed Smart Contract Execution

Currently, smart contracts require a triggering event to execute. Some centralized services exist to schedule triggers, such as the Ethereum Alarm Clock[4]. Block Collider's multichain builds in a guarantee of future contract execution into the chain, so that no centralized or third party service is required for this essential feature.

---

2 MULTICHAIN MECHANICS

2.1 Weaving Chains

The key architectural thrust behind Block Collider's multichain technology is the encapsulation of the current state of each of the bridged chains into the Block Collider multichain. That is, at any time t, the most current Block Collider block being mined (or having just been mined) references the most recent block in each of the supported (or "bridged") chains.

Background: Standard Blockchains

In common blockchains (including Bitcoin, Ethereum, and most others), a sequence of blocks are chained together to avoid double spending and unauthorized credits/debits of value. Each block is a combination of the Merkle root transaction data, a state root in some chains, the header hash, and a reference to a previous block's header hash. The block itself can be uniquely referenced by its header hash, so this hash is used as a caching key or query key.

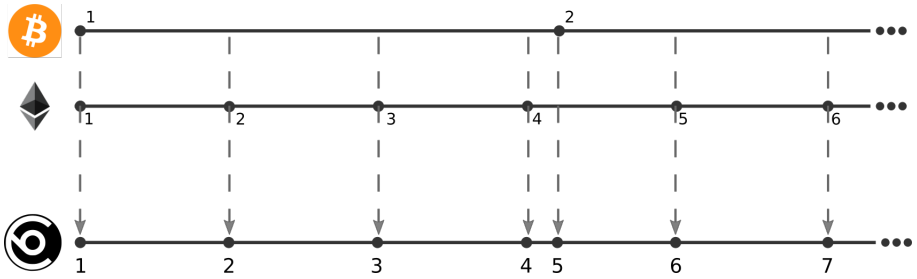
```
BTC Block Hash #0:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

BTC Block Hash #1:
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
```

Each of these hashes forms a sequence of block headers with the most recent validated block in the chain being the largest "block number" and head of the chain. At the time of writing this paper, according to CoinMarketCap there are 609 blockchains which mine, each issuing these hashes at varying speeds across a network of thousands of machines[8].

"Base Tuples": Unifying the Latest Blocks on each Bridged Chain

In the Block Collider blockchain, every block references the head block from each the bridged chains — this tuple is called the block's "base tuple". More precisely, a Collider block's base tuple can reference any recent valid block on a bridged chain whose parent has been referenced in a previous Collider block's base tuple. This lets the Collider chain serve as a unifying chain for all of the bridged chains.

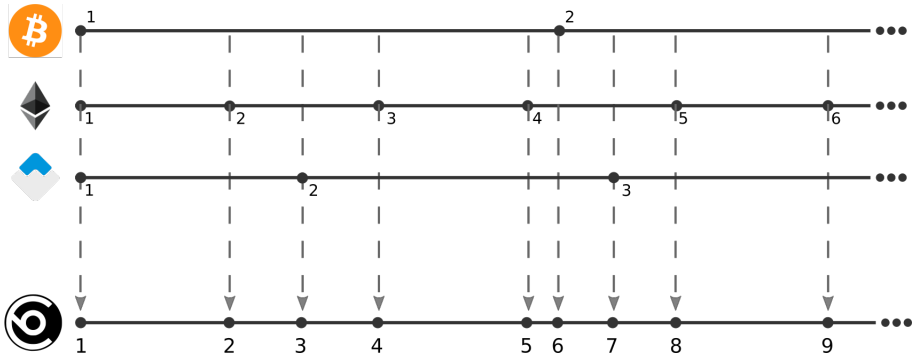
Because of the combinatorial nature of base tuples. the Block Collider blockchain is consistently faster than the fastest bridged blockchain. For example, since there is currently a new Ethereum block every 30 seconds[9] and a new Bitcoin block every 9.2 minutes[7], a Block Collider multichain from those two chains would have a new block for every new combination of blocks, or approximately every 28 seconds. Consider the following example (not to scale):



Notice that in this example Ethereum Block 4 is reused once — reuse of blocks in base tuples is a common occurrence, ensuring that:

```
Block Collider block(BTC block 1, ETH block 4) < Block Collider block(BTC block 2, ETH block 4)
```

In the above example, the Ethereum blockchain at ETH block 4 is an instance of Block Collider being the fastest chain. This concept becomes clearer when we add a third blockchain into the mix. In the following example, for every two Ethereum blocks one WAVES block is issued:



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

Keep in mind that these tables represent the same period of elapsed time. Note the increased block issuance rate of the Block Collider chain, in that the total blocks went from 7 in the first example to 9 in the second example. The addition of another blockchain (in this case Waves) increases the number of combinations in Block Collider.

Block Velocity

Since the Block Collider multichain issues a new block each time any bridged chain issues a new block, the number of new Block Collider blocks is the sum of the number of new blocks in all bridged chains. This means that the block velocity (that is, the number of blocks mined in a given interval, V) of the Block Collider multichain is approximately the sum of the block velocity of each of the supported chains (modulo the time it takes for new bridged chain blocks to get hashed into the Collider multichain). Since the block interval (the time between blocks, T) is the inverse of the velocity ($T = \frac{1}{V}$), this translates to a harmonic relation between the Block Collider multichain and its bridged chains. That is, for each bridged blockchain i of the Block Collider multichain:

$$V_{BC} \approx \sum_i V_i$$

$$\frac{1}{T_{BC}} \approx \sum_i \frac{1}{T_i}$$

By adjusting the difficulty threshold for the computation to mine a block, the computational complexity from additional chains can be controlled to keep latency low with equivalent hashrate, even as the velocity necessarily increases.

In the previous example, miners in the first iteration of the Block Collider formation, "BTC + ETH", are looking for "base pairs" while in the second they are looking for "base triples" for "BTC + ETH + WAVES" and so on. In this way, the Collider multichain leverages the variance in bridged chains to create a singular rapidly moving blockchain while supporting trusted inter-block issuance operations which are especially useful for high speed asset trades or operations.

Due to the variability of block discovery on all blockchains, where Ethereum for instance ranges from 6 seconds to 2 minutes and Bitcoin commonly ranges from 5 to 15 minutes, it will be impossibly difficult for miners to try to preempt combinations that cause the Block Collider blockchain sequence to favor one chain. This drastically increases the computational difficulty of the multichain thwarting attacks that involve shifting mining power on the Block Collider.

Decreasing the block time has consequences for stale rates and centralization incentives. To combat these issues, Block Collider splits block mining from transaction mining. This concept will be covered in the next section.

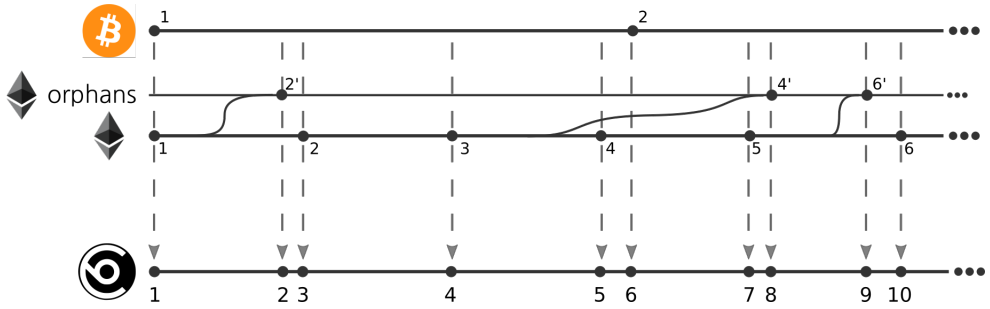
2.2 Multichain Conflicts

Because each block on the Collider references blocks on supported chains, when there is disagreement on a supported chain as to which block is the head, Block Collider miners will inherit some of that conflict. One multichain strategy would be to let these conflicts pass through to the Collider, letting the Collider chain split and resolve as any of its chains split and resolve. However, this would create a very high floor on the Collider stale rate, would induce discontinuous block miner incentives, and would create additional issues around ensuring that the split resolves.

Instead, the Collider allows for inclusion into a base tuple any recent valid block (including orphans and uncles) whose parent has previously been referenced in a base tuple. "Recency" as used here

means that the block depth is not substantially less than the highest depth block that has been observed on that chain, with the threshold for recency varying for each bridged chain (and determined by each chain's uncle / orphan strategy).

For the purposes of computing the resultant Collider chain velocity, this orphan permissiveness increases the effective block velocity of bridged chains by a factor determined by that chain's orphan rate. Consider the following example: a BC multichain is constructed on top of BTC and ETH chains, and in every even-numbered ETH block there is a depth-1 disagreement. Let " ' " denote that a block becomes an orphan, e.g. " 2' ", and note that depth-1 disagreements imply that every block has a non-orphan parent; then we can observe the following:



Note that either the orphan or the non-orphan ETH block can appear first in the BC chain, since it is not known which is which until the split is resolved. Note also that there is limited "backtracking" allowed, but that for low stale rates such backtracking is highly localized. Finally, note the effective increased BC block velocity; since ETH in this example has a stale rate of $\frac{1}{3}$, its effective velocity is increased by $(1-\frac{1}{3})^{-1} = 1.5$, or a 50% increase.

---

3 MINING ON THE COLLIDER

3.1 Consensus Approach: "Proof of Distance"

Block Collider uses a modified version of Nakamoto consensus to determine the next head block; that is, at its core:

> Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously,

> some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. [15]

Block Collider modifies this by introducing a new algorithm for the computational challenge required to mine a new block, which is based on string edit distance and is described later in this section. This challenge generalizes the idea of filtering for hashes below a certain threshold into the idea of filtering for hashes within some distance of a reference set — hence, "Proof of Distance".

A Block Collider block, like other blockchains, includes transactions and references to previous blocks and proofs in the form other other blockchain block headers in order to validate the work done on each block. However, unlike other blockchains, Block Collider blocks do not have a fixed number of transactions. Instead, each block has a "distance balance" which the sum of the block's transaction distances must stay below, which is based on the amount of Emblems the block miner owns.

Emblem Block Size Bonus

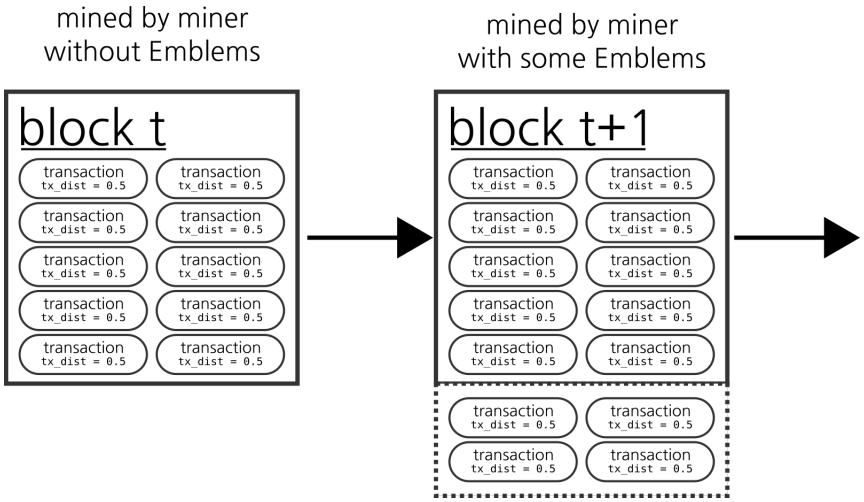
Emblems are the crypto macro-asset issued by Block Collider. Block miners are granted a block size bonus based on the amount Emblems they hold, by allowing additional space for transactions in a block, which in turn increases the transaction fees which they can collect. By analogy, imagine a mining cart—the more the block miner can load into the cart, the larger their payout might potentially be if gold is found. Emblems allow block miners to have bigger carts.

In comparison, Bitcoin and Ethereum blocks can only accept a certain amount of transactions due to their size or gas limits. While some limit is necessary to avoid network congestion from enormous blocks, arbitrary fixed limits are clearly a suboptimal answer. Variable block sizes allow for additional incentive alignment, letting those miners more invested in the network (literally) produce more from their work. Moreover, fixed block sizes force transactions to be ranked purely by fees, whereas the Block Collider mechanism allows for more flexible side-channels to influence priority via the transaction's "transaction distance".

With the Block Collider multichain, each block is capped by a maximum sum of "transaction distances" (explained in more detail later in this section) contained within each transaction. This means that if the max sum distance for the block is 5, then the miner would be able to accept 10 transactions of distance 0.5 ($0.5 \cdot 10 = 5$). Thus, transactions with lower distances have a greater chance of getting into a block with minimal fees, so that a user can pre-mine the distance and increase the probability of inclusion

in a block even with lower fees. Otherwise, a transaction might include no work and a significant fee which incentivizes the miner to allocate some of its mining power to adding the transaction.

Whether or not the user pre-mines their transaction, Emblems increase the block miner's max sum distance that can be included, for example from 10 to 12 in the following figure:



Emblems do not increase the probability of the miner finding the next block; the same distance score must be found regardless of the number of transactions accepted in the block. Additionally, the Emblem bonus is sublinear (that is, there are diminishing bonus returns for Emblem ownership), which balances the economic incentive against centralization (as the marginal utility of Emblems will be highest for those with fewer Emblems).

Dynamic Difficulty Threshold

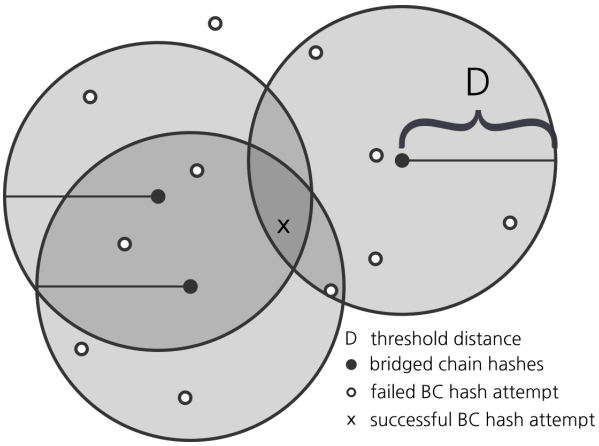
Because the Block Collider multichain's block interval is dependent on the block interval of its bridged chains, guaranteeing a block interval is infeasible. Instead, there are target delay periods for each of the six planned forks, targeting delays of 5.5 seconds, 3.5 seconds, 1.5 seconds, and 0.5 seconds. That is, at first, the Collider multichain is targeted to release a new block approximately 5.5 seconds lagged behind the most recent block of any of the bridged blockchains.

The challenge difficulty threshold is dynamically adjusted to fit these target windows. If a solution has not been found when an additional new block from the same bridged chain is observed, there is a temporary threshold decrease, making it easier for Collider miners to quickly catch up to blockchains issuing blocks at a faster-than-expected rate. In addition to providing an adjustment for exceptional block rates on a bridged chain, this also smooths situations when the edit distance is particularly difficult to find (such as, by geometric analogy, when the distances between the hashes from the bridged chains are distal).

3.2 The Edit Distance Computational Challenge

The "mining" of the Collider multichain is the computational challenge of finding a hash that satisfies a minimum edit distance between the hashes of member chains, its transactions, and its previous block. Block Collider uses the Cosine Similarity algorithm[17] to score the similarity between two hashes.

Traditional hash-based approaches can be thought of as finding a threshold on the distance between the discovered hash, and the arbitrary reference point of "zero" — that is, any hash within some distance D of zero is also less than some hash threshold (also D). Edit distance expands this implicit notion of distance into multidimensional space. Because edit distance and more traditional proof-of-work challenges share this fundamental core, both approaches can easily adjust computational difficulty by moving their distance threshold.



To satisfy Block Collider's computational challenge for block mining, a block miner must continue to choose random nonces and compute:

```
hash_attempt := hash(miner_public_key + nonce)
```

The challenge can terminate when the result satisfies (for the two-chain case):

```
RO(hash_attempt, BTC block hash) < D && RO(hash_attempt, ETH block hash) < D
```

or, equivalently:

```
max(RO(hash_attempt, BTC block hash), RO(hash_attempt, ETH block hash)) < D
```

Once a block miner finds a nonce whose resultant hash satisfies the constraint threshold, they propagate their solution to the network to win the block reward, which includes some of the fees allocated in

the transactions submitted to that block. Each Block Collider block contains references to the previous block and the header-states of any relevant blockchains used in its construction.

Edit Distance	Traditional PoW Distance
measured from reference points	measured from zero
"multivariate"	"univariate"
threshold easily adjusted	threshold easily adjusted

Edit Distance in Block Mining: Example

Imagine a three-blockchain Collider multichain. We would then start with three strings, each representing the header hash of a block from another blockchain:

```
BTC:      000000000000000006abfe31e59af9f81b3fc84a1a25a8fdc095e429dc6dffa
ETH:    0x73413ff99013f6007b72e299aee87da63311602ae4dfb1466b254b7c89b8e1bd
NEO:      0b58e3e1980eb79c293ee1d047997c5a7092da8d49813c2407e90f85e0ba1f9e
```

Imagine the current threshold on this Collider multichain is 0.29. To mine a new block in the root blockchain, the block miner would iterate through a random charset or number, hashing strings until it finds a hash that is below 0.29 for all of the blocks. With a single web-worker on an Intel Core i7 processor, a prototype miner found the following solution in 32.6 seconds:

```
Solution:      c53a147e80b2ae87c50d62dfdc82501d0405c9734d0daf6197918f182ca6c7f5
```

Edit Distance in Transaction Mining

In the case of transaction mining, a transaction miner must first compute the transaction data, then must try successive random nonces:

```
hash_target := hash(transaction_data)
hash_attempt := hash(miner_public_key + nonce)
```

The transaction edit distance is then the distance between the `hash_attempt` (based on the miner work) and the `hash_target` transaction ID (TXID):

```
tx_dist := R0(hash_attempt, hash_target) * byte_size(transaction_data)
```

Each block can only include up to some sum of transaction distances (`tx_dist`), determined by the amount of Emblems the block miner has access to. A transaction miner may continue to mine a transaction for a lower distance, for a higher chance of being included in a block, or may simply broadcast its solution and wait for inclusion. The implications of splitting transaction mining from block mining are discussed in the previous section.

Advantages of Edit Distance

From an intuitive standpoint, taking a hash of data transforms the data into an irrecoverably different kind of space — that is the intent of hashes, which are also known as "trapdoor functions". Since the Collider chain is generating its own hash, which references other hashes, for simplicity's sake no additional space needs to be defined, and all operations can take place between hashes without entering any trapdoors. This commitment to elegance allows for interesting geometric interpretations of hash space, since Cosine Similarity is symmetric and is a well-formed metric.

Moreover, as byproduct of computing an edit distance, the algorithm generates a description of how to edit one string to transform it into another, so that validating the edit distance is computationally simpler than computing it. This asymmetry compounds the asymmetry already present in guessing points in hash space to find one within a suitable distance, which is the key feature of computation challenges.

Lastly, whereas many hash algorithms are intentionally designed to be computationally expensive with no other purpose, edit distance is actually a useful problem to solve. If optimizations are found for inner loops of artificially constructed computational challenges, no great progress has been made. By putting a real, useful problem at the core of Block Collider's computational challenge, any resultant work towards optimizing solutions also benefits the rest of the computer science community in the form of better core algorithms.

	Edit Distance computational challenge grants...
1.	Natural multidimensional, geometric extension of minimizing a hash
2.	Increased asymmetry in mining versus validation
3.	Altruistically meaningful algorithm to optimize

3.3 NRG

NRG (Non-Relational Graphs) is the on-chain currency mined on the Block Collider. It is the primary fee used for conducting transactions and awarding miners, similar to "Gas" on Ethereum, except split into its own token. Like Emblems, NRG has a fixed supply; the total NRG available is around 9.8 billion. Unlike Emblems, NRG can be mined. NRG mining rewards diminish over time so that mining can continue ad infinitum on its fixed supply.

3.4 Transaction Mining

To mine transactions, a transaction miner must first evaluate any required computation for the transaction. A transaction miner then finds a nonce which, combined with the transaction miner's public key, is some edit distance away from hash of the transaction data (explained in more depth in the above section on "The Edit Distance Computational Challenge"). A transaction miner may continue to mine a transaction for a lower distance, for a higher chance of being included soon in a block, or may simply broadcast its solution and wait for inclusion. Thus, the transaction miner needs to be aware of going market rates for transaction inclusion to maximize fees gathered.

Block Mining	Transaction Mining
One winner per block	Many winners per block
Contributes to network security	Contributes to network throughput
Fees in NRG	Fees in NRG
Based on an edit distance challenge	Based on an edit distance challenge
Tilts to network speed and hashing power	Tilts to network speed and performant databases

If a transaction miner has non-fee interests in a transaction (for instance, if the transaction miner is one of the transacting parties, or if the transaction miner has been paid in a side-channel), the transaction miner can continue to mine a transaction distance to be even lower, so that the fees paid within the Collider chain can be substituted with computational power. This simple mechanism for out-of-band incentives enables a new kind of cryptographic service provider, which can use computational power to ensure that transactions are posted, because transactions with smaller transaction distances are more likely to enter a block even without high fees.

Second, yet another service provider is enabled, as some transactions fall through the cracks and are not mined. Small miners, who may not have the hardware for profitably working on blocks, can participate in the network by listening for otherwise missed transactions (likely from lite-clients), mining them, and subsequently broadcasting the transaction to all their peers to claim part of the fee included in the transaction.

Advantages of Splitting Transaction Mining from Block Mining

Whereas some other chains are exploring the strategy of including work from uncles (blocks in competition with a recent block in the chain) to gain some advantages from stale blocks[11][18][13], Block Collider gains similar advantages by separating transaction mining from block mining. While block miners compete over the more scarce real estate of winning the next block, transaction miners compete in a much less crowded space with lower chance of conflict, which decreases the amount of work replication between them. So although Block Collider does not fold in work from stale blocks, the amount of computational work lost from stale blocks is greatly reduced compared to other chains.

Separate Transaction Mining means...
1. Reduced duplication of work, leading to increased efficiency
2. Increased barrier to network centralization
3. Opportunity for miner specialization, leading to increased efficiency

From an economic standpoint, one can think of this separation as splitting a vertically integrated industry — by allowing for competition in two spaces, there is reduced risk of centralization, since an actor would have to win the centralization game at both levels. Especially because transaction mining and block mining have very different fundamental requirements (in memory, in computational type, and in architecture), splitting these functions allows for greater efficiency through specialization.

---

4 MULTICHAIN TRANSACTION DYNAMICS

Over the past year there have been several attempts to create a "decentralized marketplace", such as Token from Coinbase[5], Swap[6], ShapeShift[1], and ox[19]. While well-intentioned and not without

new features for trading, they are severely limited due to their dependency on Ethereum, and thus to Ethereum's block speed. Currently, the experience requires that a user wait for the next Ethereum block to pick up their submission of the intent to trade, and then at least one more block for the opposite party to accept that intent and complete the trade. If each Ethereum block takes 30 seconds, this process can take minutes. This also assumes the unlikely event that the transactions of either party are picked up by miners in the immediate block following their transaction. On the other hand, so far any solutions not built on the Ethereum chain have been centralized.

With the foundation described in the previous sections in place, the Block Collider multichain can host multichain transactions far more rapidly, and in a truly decentralized manner. Services that use the Block Collider will be able to serve order books with significantly faster updates, far faster than the block generation frequency of a bridged blockchain. They will also be able to facilitate cross-blockchain trades instead of "token swaps", which at the moment are entirely on the Ethereum blockchain or conducted on centralized exchanges.

4.1 Transaction Basics

Transactions for the Collider are stored on a distributed hash table (DHT), which miners use to synchronize with other nodes and validate work. Nodes are only expected to synchronize with this table to avoid the usage of bloom filters which delay blockchains due to their inability to reference partial ranges. The storage method proposed is very similar to IPFS[10], in that a client can store all or some of the chain locally. Since the Block Collider multichain is synchronizing with many blockchains, it retains or has access to the state of each chain temporarily. This allows the Collider to set up transactions which execute when a particular event occurs on one of the bridged chains.

Block rovers (processes which discover and distribute blocks, discussed in the following section) are the ideal tool for broadcasting transactions intended to execute on each member blockchain. Miners operating these block rovers will sign the submission of the transaction which validates their claim to the fee. As the network expands, we expect that it will be economical for rovers and miners to split, which is why this process requires only the valid private signature and not a base pair.

4.2 Marked Tokens

The Block Collider multichain has marked-token currencies, which is a unit of value for each bridged chain. These marked tokens are only available on chains that support tokenized assets or side-chains and could be compared to "colored coins"[3].

For example, on Ethereum, the Collider uses Marked Ethereum (or M-ETH) which is an Ethereum ERC20 token. Each transaction this token is a part of is automatically a valid part of the Block Collider multichain. The marked tokens are observed by rovers (discussed in the following section) and are used to speed up peer synchronization. The following would be a transaction that, even though executed on Ethereum, could be retrieved from the Block Collider multichain.

```
0xd12Cd8A37F074e7eAFae618C986Ff825666198bd Transferred:TXID -23 M-ETH
0xBB9bc244D798123fDe783fCc1C72d3Bb8C189413 +22.999 M-ETH
```

Using bytes to identify the token is not unique to Block Collider; it is the same way the Ethereum blockchain identifies that a particular token has been transferred. Any transaction or block can be passed to the Block Collider. This process in theory could be used if a token of a blockchain became more valuable than the chain itself, and subsequently the miners of the Block Collider could merge it in as its own chain using the byte flag as differentiator from its host chain.

4.3 Promises

On the Block Collider multichain, promises are encrypted transactions that decrypt and run when an event on another chain is observed. There are two key components to a Collider promise: the private data and the bit filter. The private data is a transaction that is intended to be executed at a future time, which is encrypted. This could be data-heavy, such as a document dump, or more computation heavy, such as a smart contract to execute. The bit filter signifies where to look for the decryption key to decrypt the transaction. The bit filter must be a simple bit slice, potentially given some constraints, of a transaction hash on a bridged chain.

A transaction miner intending to mine a promise would watch the identified bridged chain until the bit filter found a slice that matched, and was able to decrypt the private data. It would then decrypt the private data into a transaction, and post that transaction, claiming fees both from the original promise and optionally from the bridged blockchain transaction.

Promise Example

Promises on Block Collider's multichain easily allow a fully decentralized implementation of Wikileaks. Imagine Alice has information about her employer that she believes should be made public, and wants to ensure that, in the case that a controlled release is not possible, that a document dump will still occur. Alice could put an encrypted copy online and use a Collider promise for key dissemination. Specifically, Alice could set up a promise that would stay silent as long as some data was posted to any bridged chain, signed with her private key. If she stopped her "heartbeat" broadcast, the promise would decrypt and post a transaction with the key for the private data to the Collider or to any bridged chain.

4.4 Callbacks

Callbacks are an incentive-compatible way to execute multichain transactions between users. They are the natural evolution of "atomic swaps", which can not only trade coins, but can execute arbitrary transactions based on conditions or on transactions on other blockchains.

Callbacks are executed in two stages; setup and fulfillment. Each action after the setup stage is ensured with collateral, offered up by whichever party has the opportunity to defect and walk away. In this way, if one party breaks off this multi-stage protocol, the remaining party is made whole with the collateral from the defecting party.

In the setup stage, first the callback initiator posts a callback transaction, which sets up and funds a bonus address, and which provides partial information to set up collateral addresses. The bonus address is funded and covers some of the fees for miners over the course of the transaction. The collateral address is where a sufficient store of value is kept, such that if one actor backs out of the transaction, the counterparty can always be made whole by the amount in the collateral account, and such that the backing out is never in the economic best interest of either party.

In response to the initiating callback transaction, then, a respondent posts a responding callback transaction, which funds a bonus address, and provides partial information to set up collateral addresses. The combination of information from both parties fully specifies the collateral addresses, which are locked and unlocked based on the current state of the transaction[16].

In the fulfillment stage, the initiator and respondent alternate partially (or fully) fulfilling the transactions. For the protocol to be incentive-compatible, the collateral put up by each collateral must cancel

out any potential loss by the opposite party. Naively, the collateral must be at least as valuable as whatever is being transferred to maintain incentive compatibility. However, by allowing partial fulfillment, the collateral can be up to k times less valuable than the entire transaction, where k is the number of partial pieces the full transaction is broken up into. In this way, there is a natural trade-off between the speed of execution and the amount of collateral either party is willing to offer as collateral.

Each piece of the fulfillment stage includes an expiration timer. If the timer expires before the appropriate party makes the agreed-upon full or partial transfer, they are considered to have defected, and their collateral is forfeit. The exact dynamics are open to customization, so that in addition to being made whole, there could be an extra convenience fee for defecting on a counterparty.

Callback Example

Imagine Bob wants to offer to trade `5.0 ETH` for `0.2 BTC`. Bob creates a callback transaction, which funds a bonus address, which is to fund the mining fees covered by the protocol, and provides partial information to set up a collateral address (C_{Bob}). Bob proposes that this callback occur in 5 pieces, so his collateral address must cover `1.0 ETH` (since `5.0ETH / 5 pieces = 1.0ETH`).

Imagine Alice and Carol both want to become counterparties to that transaction. Both Alice and Carol submit transactions responding to Bob's callback transaction, which attempt to fund a bonus address, and to fund a collateral address (C_{Alice}, C_{Carol}). A block miner picks one (let's say Alice, without loss of generality). Carol's balance is not affected since her response was not chosen.

Now that the setup is completed, Bob and Alice move to the fulfillment stage, both with at least $\frac{1}{5}$ of the value in their collateral account. For the first piece, Bob transfers one fifth of what he promised (that is, `1.0 ETH`) to Alice's account. His transfer unlocks the collateral in his account, and locks the collateral in Alice's collateral account. Then, Alice transfers one fifth (or `0.04 BTC`) to Bob's account, and that transfer unlocks her collateral account, and re-locks Bob's collateral account. This continues piece by piece until the entire transaction is complete.

If at any stage either Bob or Alice does not continue the transaction as expected, there is clearly enough in the defector's collateral account to provide restitution for the cooperating party, who can then complete the transaction elsewhere.

	Step	ETH_{Bob}	BTC_{Bob}	ETH_{Alice}	ETC_{Alice}	C_{Bob}	C_{Alice}
1	Bob creates callback transaction	**6 ETH**	**0 BTC**	**0 ETH**	**0.24 BTC**	—	—
2	Alice creates response callback	6 ETH	0 BTC	0 ETH	**0.2 BTC**	0 ETH	**0.04 BTC**
3	Bob funds his collateral	**5 ETH**	0 BTC	0 ETH	0.2 BTC	**1 ETH**	0.04 BTC
4	Bob transfers first piece to Alice	**4 ETH**	0 BTC	**1 ETH**	0.2 BTC	1 ETH*	0.04 BTC
5	Alice transfers first piece to Bob	4 ETH	**0.04 BTC**	1 ETH	**0.16 BTC**	1 ETH	0.04 BTC
6	Alice transfers second piece to Bob	4 ETH	**0.08 BTC**	1 ETH	**0.12 BTC**	1 ETH	0.04 BTC*
7	Bob transfers second piece to Alice	**3 ETH**	0.08 BTC	**2 ETH**	0.12 BTC	1 ETH	0.04 BTC
8	Alice transfers third piece to Bob	3 ETH	**0.12 BTC**	2 ETH	**0.08 BTC**	1 ETH	0.04 BTC*
9	Bob transfers third piece of to Alice	**2 ETH**	0.12 BTC	**3 ETH**	0.08 BTC	1 ETH	0.04 BTC
10	Alice transfers fourth piece of to Bob	2 ETH	**0.16 BTC**	3 ETH	**0.04 BTC**	1 ETH	0.04 BTC*
11	Bob transfers fourth piece of to Alice	**1 ETH**	0.16 BTC	**4 ETH**	0.04 BTC	1 ETH	0.04 BTC
11	Bob transfers final piece of to Alice	**0 ETH**	0.16 BTC	**5 ETH**	0.04 BTC	1 ETH*	0.04 BTC
12	Alice transfers final piece of to Bob	0 ETH	**0.2 BTC**	5 ETH	**0 BTC**	1 ETH*	0.04 BTC*
13	Alice reclaims her collateral	0 ETH	0.2 BTC	5 ETH	**0.04 BTC**	1 ETH*	**0 BTC**
14	Bob reclaims his collateral	**1 ETH**	0.2 BTC	5 ETH	0.04 BTC	**0 ETH**	0 BTC

Note that an unlocked collateral address (noted with a $*$) means that, in case the next step of the transaction times out, the actor who put up the collateral may reclaim it. Otherwise, that actor cannot reclaim that collateral. Note also that, at every stage,

$$\frac{BTC_{Bob,t}}{BTC_{Bob,\text{total receive planned}}} + \frac{ETH_{Bob,t} + ETH_{Bob\ \text{unlocked collateral},t}}{ETH_{Bob,\text{total sent planned}}} = 1$$

...so that if Alice halts the transaction at any step, Bob is not worse off than having received a pro-rated completion of the transaction. The converse, for Alice, also holds. However, due to the locked nature of the collateral, any party which halts the transaction loses their collateral, and is thus significantly worse off. The larger the collateral required for the transaction, the more a party stands to lose by halting the transaction.

Like any complex communication protocol, it is not expected that users will have to perform these steps themselves. The Collider multichain will provide the building blocks for these transaction, and the Block Collider team will release software for easy interaction with this protocol.

5 INSTRUMENTAL INNOVATIONS

In striving to develop technology that can achieve results beyond the current state of the art, the Block Collider team has created new approaches and concepts in many key areas. The following are a few of our favorites.

5.1 Block Rovers

The Block Collider chain is built from the myriad of blocks being issued by other blockchains through a process that rapidly distributes and fuses them together, incentivizes truthful work, and gives back to the community by seeding chains to new client nodes, even if the node itself is not synchronizing the Block Colliders blockchain.

To begin the process of fusing chains together, Block Collider introduces, in addition to miners, new network-based workers called "block rovers" which assist miners in relaying blocks from other blockchains back to the miners for processing. From the beginning, rovers are automatically built into the mining applications provided by the Block Collider core developers and development community.

To illustrate, a block rover traversing the Bitcoin blockchain is constantly seeking new blocks at the head of the chain in order to relay these blocks back to the miners. The rover seeds the blocks from the Bitcoin blockchain in the same way a traditional Bitcoin node might join and participate in the network. The key difference is that a block rover will maintain a group of over a hundred remote clients from which to seed blocks instead of, in Ethereum's case, a default 25. Rovers are setup for each member chain like Waves, Ethereum, and NEO.

Because of Block Collider's multichain nature, block miners are incentivized to run block rovers so that their neighborhood in the network does not lag behind other neighborhoods. The effective network for Block Collider includes all of the bridged chains' networks, layered on top of each other, so Block Collider miners are particularly incentivized to spread blocks around. Defecting and hoarding blocks is not an advantageous strategy unless a miner's neighborhood is coincident with the fastest neighborhood in the network of each supported chain, which will almost certainly not be the case for any miner.

5.2 The FIX Protocol

In developing new financial technologies, the pursuit of low latency trade orderbook data and trade execution has created rapid innovation for "bare metal" high-performance computer and networking infrastructure. One of the most reusable elements of this is the Financial Information eXchange [12] protocol, which was created for international real-time exchange of information related to the securities transactions and markets.

The Block Collider uses this protocol in two primary capacities. First, internal to Collider mining, pending transactions (including their fee and `tx_dist`) and going rates for transaction inclusion in blocks are distributed via FIX. Since the process of filling a block with transactions can be compared to the settlement of an order book, up to date transaction distances are necessary to insure efficient placement of transactions in blocks. Second, external to Collider mining, the FIX protocol acts as an ecosystem-wide data feed for all of the blockchains connected to the Block Collider. The data feed serves as a simple entry point for institutional investors to more easily price market events, volume, and tick-level data in a timely fashion with a protocol already integrated into their on-premise systems.

5.3 Optimized Block Routing

On blockchains, transactions must of course take place in a secured fashion, without relying on any trust except that which is cryptographically ensured. However, there are situations in which a second level, looser understanding of trust can be used to help optimize the network functioning.

Block Collider builds into the network protocol an additional layer of probabilistic "trust", which optimizes network flows based on verifiable claims that other nodes make on the state of the network and their own information. There is a soft incentive for nodes to participate truthfully, in that participation as an honest user increases the speed at which a node will receive blocks and get its own blocks propagated in the network.

---

6 LOOKING TO THE FUTURE

Going forward, the Block Collider team expects the Collider mutlichain to evolve and grow. Change is especially difficult, however, in decentralized consensus systems designed to be inherently trustless. The following are our expectations for changes that will be built into the software we distribute, and the direction in which we intend to progress.

6.1 Protocol Considerations for Development

Scaling to More Bridged Chains

The Block Collider is designed to add new blockchains easily, in that each new blockchain is intended to be an insignificant increase to the load placed on miners or rovers. The computational challenge will remain the same, except with additional terms in the constraint. For example, going from two to three chains, the block mining threshold expands like so:

```
max(RO(hash_attempt, BTC block hash), RO(hash_attempt, ETH block hash)) < D
```

```
max(RO(hash_attempt, BTC block hash), RO(hash_attempt, ETH block hash),
  RO(hash_attempt, WAVES block hash)) < D
```

With the addition of new blockchains, the difficulty threshold will be adjusted to maintain difficulty continuity.

Even if a bridged chain experiences a cataclysmic event, causing it to cease to emit blocks, the Collider will still function without disruption. The Collider is designed so that it can safely secure transactions as long as it is still assimilating two or more blockchains. The continuing stream of Collider blocks requires only that new, unseen blocks are observed and processed by miners. A given blockchain might go offline, so that until the assimilation council (discussed below) removes it, the Collider would only slow down slightly due to a decrease in the number of new blocks available for inclusion.

Planned Hard Forks

At launch, the Block Collider will support six blockchains. The sixth chain is not listed on the website, and will secretly run parallel to the other blockchains on private nodes to avoid market effects influencing pricing of the chain.

For the first three years after the mainnet, hard forks will be pushed to the community a maximum of six time. These forks will include bug fixes, and compatibility for new blockchains, efficiency improvements, and some hyperparameter changes (such as reducing the target delay after observing new blocks). By the end of these forks, a voting protocol will have been tested and confirmed as the primary way of governing the Collider multichain on a perpetual basis.

Evolution Mode and Feature Development

Once the initial six blockchains have been deployed to the Collider multichain and the core protocol passes the incubation window of two years, the protocol switches to an "Evolution Mode". This is a stage which includes a three month voting period during which new blockchains can be voted into the Collider, by simple majority, and unwanted blockchains can be voted out, by two-thirds majority.

In addition, Evolution Mode allows "architect voting". An architect is a public address that is associated with a project or proposal. This could be a request for funding to develop a new feature or change a previous feature. To submit a project, the owner must stake an amount of Emblems above some threshold.

Evolution Mode serves three purposes. First, it gives Emblem owners a stake in the evolution of the chain. Second, it allows the Collider to adopt new features from other chains through a democratic process. This also allows the chain to move with large scale changes in the political environment or access to new fiat markets. Finally, it allows the Block Collider to create features and organically grow involvement from the community. A similar program can be found in the Dash Development Fund, which is perhaps an ideal example of this behavior[2].

Voting

In the event of an emergency, there is a version flag which can be triggered by miners to migrate to an alternate chain or group of chains. The version flag, like the one used in Bitcoin, only supports a single digit numeral, signifying the gravity of the change. It is a not a "break the glass" event, but does

give miners the ability to move away from chains that have put in a state of disrepair such that it is significantly negatively impacting the Block Collider.

6.2 Vision and Future Direction

Recent developments have seen a tremendous surge in interest and in technical advancement in the field of using cryptography to solve coordination problems. Any limits to implications for the future of society and economic systems are yet undiscovered. This may very well herald a new paradigm, where individuals, simply by the nature of having access to private information, can be cryptographically assured of their rights, and of their freedom to choose and act in the world.

The industry as we know it, however, is strongly siloed. While extant systems grant users freedom within their domain, users are still confined and must stay within that system. Many solutions to the multichain problem rely on centralization, such as via validators, which is fundamentally dissonant both with the values and with the advantages of the crypto industry. By weaving together disparate chains into the Block Collider multichain in a truly decentralized way, we hope to enable a new level of individual choice and freedom through cryptography. In the future, we at Block Collider hope to merge in more chains, and to more tightly integrate features across chains, so that individuals can have the freest possible choice across crypto systems.

By questioning primary assumptions about blockchains — including breaking the vertical integration of block and transaction mining to enable side-channels for incentives, opening the incentive channel of block sizing via Emblem ownership, and innovating new algorithms for computational challenges, to name a few — Block Collider contributes towards continued rapid progress and fundamental innovation in the ecosystem.

The Block Collider team is dedicated to freedom through cryptography, and we hope you will join us on that journey.

REFERENCES

[1] About the exchange. Shapeshift Website.

[2] Decentralized governance system. Dash Official Website.

[3] Colored Coins protocol specification. Colored Coins Github Repo, 2015.

[4] Ethereum Alarm Clock: It begins, 2015.

[5] Coinbase to launch standalone Ethereum messaging app token. The Coin Telegraph, 2017.

[6] Introducing Swap: A protocol for decentralized peer-to-peer trading on the Ethereum blockchain. Airswap Blog, 2017.

[7] Bitcoin Block Time historical chart. BitInfoCharts, 2018.

[8] Cryptocurrency market capitalizations. CoinMarketCap Website, 2018.

[9] Ethereum Block Time historical chart. BitInfoCharts, 2018.

[10] Benet, J. IPFS - content addressed, versioned, P2P file system. IPFS Website, 2014.

[11] Buterin, V. Toward a 12-second block time. Ethereum Blog, 2014.

[12] Lamoureux, R., and Morstatt, C. Financial Information eXchange protocol specification, 1992.

[13] Lerner, S. D. Even faster block-chains with DECOR protocol. Bitslog Blog, 2014.

[14] McIlroy, M. D., Pinson, E. N., and Tague, B. A. UNIX time-sharing system: Foreword, 1978.

[15] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008.

[16] Poelstra, A. Using chains for what they're good for. Scaling Bitcoin Talk, 2017.

[17] "Cosine similarity." Wikipedia. January 26, 2018. Accessed February 10, 2018. https://en.wikipedia.org/wiki/Cosine_similarity.

[18] Sompolinsky, Y., and Zohar, A. Secure high-rate transaction processing in Bitcoin. International Association for Cryptologic Research, 2013.

[19] Warren, W., and Bandeali, A. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. 0x Whitepaper, 2017.