BLOCK COLLIDER WHITEPAPER

BLOCK COLLIDER TEAM

创建于: 2017年2月11日

修改于: 2018年1月17日

v0.9.9

目录

“程序应该只关注一个目标，并尽可能把它做好。让多个程序能够互相协同工作。”
——道格拉斯·麦克罗伊，Unix pipes的发明者。[***14***]

1 绪论

Block Collider

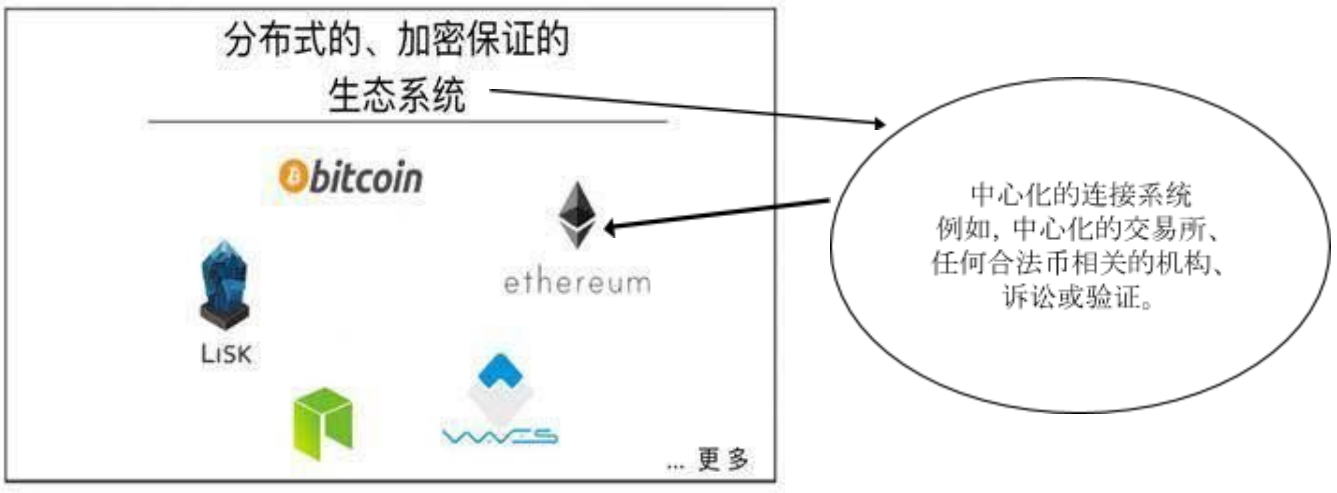
FIX

Block Collider ——

1.1

“ ”

Alice Bob Bob



Unix [14]

pipes Block Collider

1.2

Block Collider

.

. “ ” “ ”

.

.

.

.

Block Collider

1.3

Block Collider

Block Collider

Block Collider

the Ethereum Alarm Clock[4] Block Collider

2 多重链机制

2.1

Block Collider

Block Collider t Block Collider

“ ”

/

Merkle root transaction data a state root the header hash

!

&8' &JMA I , ?QF [ƈh!

ƐƐƐƐƐƐƐƐƐƐʒǂBppǁǂAƐǁŚ?Cʒpŝǁ5ʒCǂ5ŝDDIp5?Cŝp?2?pAʒI2@5Dʒ@pƐ?ǁAC2pD!

!

!

&8' &JMA I , ?QF [ʒh!

ƐƐƐƐƐƐƐƐǁ5ǂ?ǁCpǁǁp?@ŚǂŚʒBIpDŝʒʒŝIŚŝ2ǁ?DAǂƐǂŝICC52Ɛʒpʒ@@DʒǁC@pƐŝǁ!

“ ”

CoinMarketCap 609

[8]

ñ ò

Block Collider ——

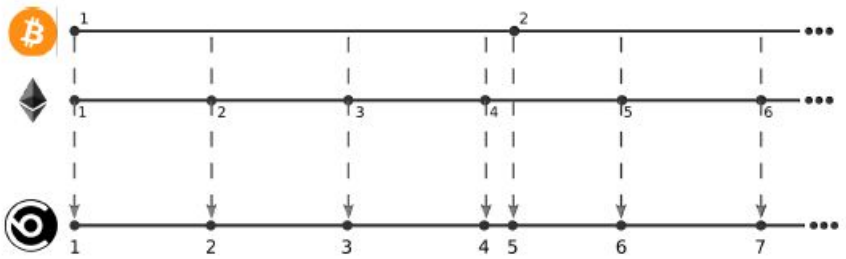
“ ” Collider

Collider Collider

Block Collider

30 9.2

Block Collider 28



4 ——

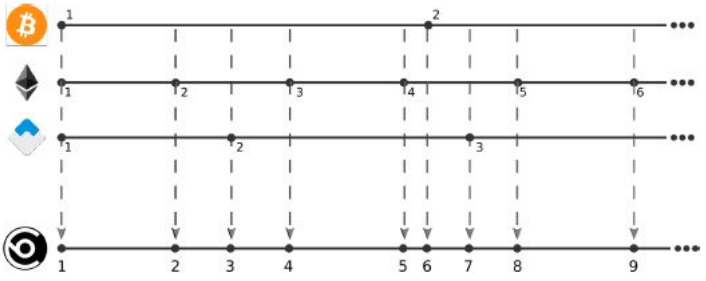
&JMAI 'MJJGBCP @JMAIi&8' @JMAI ʒ^)8, @JMAI ɔj Ǯ &JMAI 'MJJGBCP @JMAIi&8' @JMAI ƨ^)8, @JMAI ɔj!

!

)8, ɔ &JMAI ₴Collider₴

ƨ

; %:)7 !



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

Block Collider

7 9

Waves Block Collider

Block Collider Block

Collider Block Collider

Collider

T T=1/V , Block

Collider Block Collider

i

$$v_{bc} \sum_i \times v_i$$

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

Block Collider “BTC+ETH” “

base pairs ” “BTC+ETH+WAVES” “ base triples ”

Collider

6 2

5-15 Block Collider

Block

Collider

stale rate Block

Collider

2.2

Block Collider

Block Collider

Collider Collider

Collider

Collider

“ Recency ”

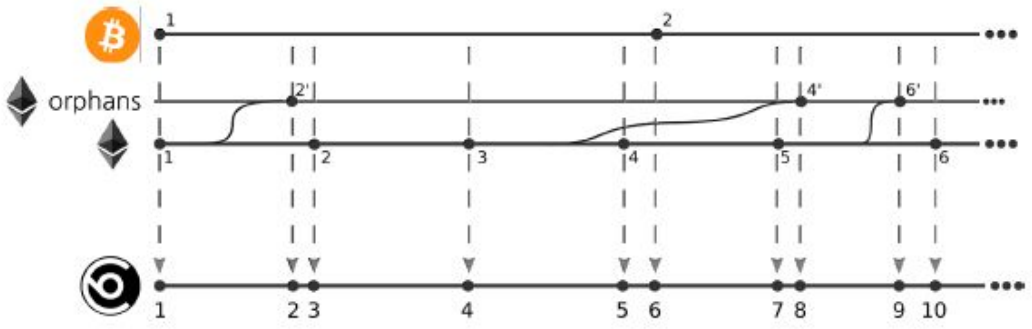
/

Collider

Block Collider

BTC ETH ETH -1 " ’ "

“2’ ” -1



ETH Block Collider

Block Collider ETH

⅓ $(1 \bar{\imath} \frac{1}{3})^{\bar{\imath} 1} = 1.5$ 50%

3 在Collider上挖矿

3.1 “ ”

Block Collider

POW

[15]

Block Collider

—— “

Proof of Distance ”

Block Collider

Block Collider

“ distance balance ”

Emblem

Block Collider

gas

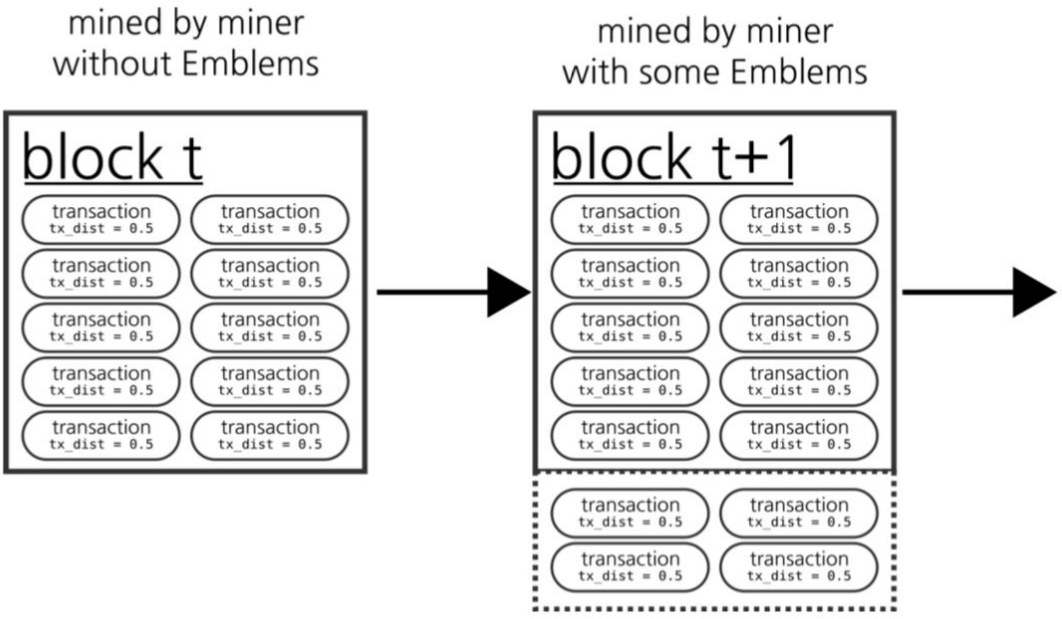
Block Collider “ ”

Block Collider “ ”

5

10 0.5 0.5 X 10 = 5

10 12



distance score

Block Collider

5.5 3.5 1.5 0.5

Collider 5.5

Collider

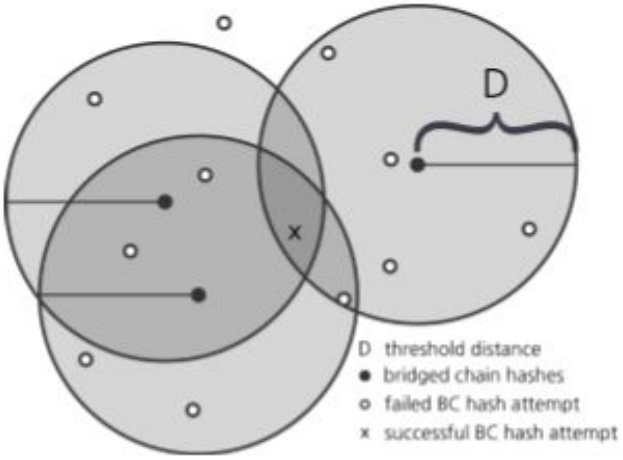
3.2

Collider

Block Collider [17]

“0”—— “0” D

D



Block Collider

hash_attempt := hash(miner_public_key + nonce)

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

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

Block Collider

Collider

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

Collider 0.29

0.29

i7 32.6

Solution: c53a147e80b2ae87c50d62dfdc82501d0405c9734d0daf6197918f182ca6c

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

the hash_attempt the hash_target ID TXID

tx_dist := RO(hash_attempt, hash_target) * byte_size(transaction_data)

tx_dist

“ ” Collider

Block Collider

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 (Non-Relational Graphs)

NRG Block Collider

“Gas” Block Collider NRG

NRG 98 NRG

NRG

3.4

“

“

NRG NRG

Collider

“ ”

Block Collider

Block Collider

……

1.

2.

3.

—

4

Coinbase Swap

ShapeShift ox

Block Collider

Block Collider

“ ”

4.1

Block Collider DHT

DHT IFPS

Collider

Block Collider

4.2

Block Collider

Collider (M-ETH)

ERC20 Block Collider

Collider

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

Block Collider

Block Collider

Block Collider

4.3

Block Collider

Collider

Collider

Alice

Alice

Collider Alice

“ ”

Block Collider

4.4

“ ”

;

[16]

لخ

k k

Bob 5 0.2 Bob

(Cᵢʲ) Bob

Bobᵉʲ

5 1 5.0 ETH / 5 = 1.0 ETH

Alice Carol Bob

(Cᵢʲ Aliceᵉʲ Carolᵉʲ)

Alice Carol

Bob Alice 1/5

Bob 1

Alice Alice Alice

0.04 BTC Bob Alice Bob

ᵉʲ Bob Alice

	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

*

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

Alice Bob

Collider

Block Collider

5

Block Collider

5.1

Block Collider
Block Collider

Block Collider
“ ”
Block Collider

100
25 Waves

Block Collider
Block Collider Block
Collider

Financial Information eXchange

FIX

Block Collider
tx_dist FIX

FIX Collider

5.3

Block Collider “ ”

6

Block Collider Collider

6.1

Block Collider

```
max(R0(hash_attempt, BTC block hash), R0(hash_attempt, ETH block hash)) < D
```

```
max(R0(hash_attempt, BTC block hash), R0(hash_attempt, ETH block hash),
  R0(hash_attempt, WAVES block hash)) < D
```

Block Collider

Block Collider

Block Collider

Block Collider

Collider

Collider

“ ”

Collider

“ ”

Collider Block Collider

Block Collider

Dash Development Fund

[2]

“ ”

Block Collider

6.2

Block Collider
Block Collider

Block
Collider

Block Collider

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.