



Merged Mining

Merged Mining



- Mining typically exclusive
- Each attempt aimed at a Bitcoin block
- How to start a new blockchain with the same Proof of Work algorithm?

Merged Mining



- Mining typically exclusive
- Each attempt aimed at a Bitcoin block
- How to start a new blockchain with the same Proof of Work algorithm?



Sha256
based PoW

BoringCoin

Sha256
based PoW

Merged Mining



- Mining typically exclusive
- Each attempt aimed at a Bitcoin block
- How to start a new blockchain with the same Proof of Work algorithm?



Sha256
based PoW

20'000'000 Tera Hash

BoringCoin

Sha256
based PoW

20 Tera Hash

Merged Mining



- Mine a Bitcoin and an Altcoin block at the same time!
- Bitcoin coinbase transaction has no input (scriptSig).

Merged Mining



- Mine a Bitcoin and an Altcoin block at the same time!
- Bitcoin coinbase transaction has no input (scriptSig).

Bitcoin

Bitcoin tx

$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$

Merged Mining



- Mine a Bitcoin and an Altcoin block at the same time!
- Bitcoin coinbase transaction has no input (scriptSig).

Bitcoin

Bitcoin tx

$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$

Altcoin

Altcoin tx

$\text{Hash}(\text{prev_alt} \mid \text{merkle_root} \mid N) < \text{target}$

Merged Mining

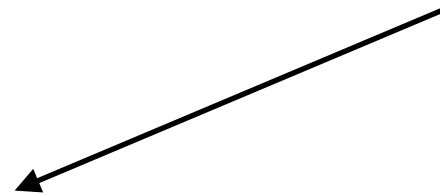


$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$

Merged Mining



$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$



tx[0] Coinbase
scriptSig: **alt header**
scriptPubKey: ...

tx[1]

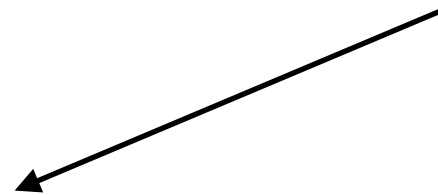
tx[2]

...

Merged Mining



$$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$$



tx[0] Coinbase
scriptSig: **alt header**
scriptPubKey: ...

tx[1]
tx[2]
...

Ignored by
Bitcoin

Merged Mining



$$\text{Hash}(\text{prev} \mid \text{merkle_root} \mid N) < \text{target}$$

tx[0] Coinbase

scriptSig: **alt header** →

scriptPubKey: ...

$$\text{Hash}(\text{prev_alt} \mid \text{merkle_root} \mid N) < \text{target}$$

Altcoin tx

tx[1]

tx[2]

...

Ignored by
Bitcoin

Merged Mining



- **Advantages**

- Easier bootstrapping of mining power

- **Disadvantages**

- Cheaper for attackers (cf. CoiledCoins)
- Inconsistency because miners might not validate transactions.

- Namecoin

- One mining pool owned 60-70% hashrate

