Merged Mining

Ondrej Sika <ondrej@ondrejsika.com>

Slush Pool (mining.bitcoin.cz)

Bitcoin

Namecoin

* first altcoin
* fork of bitcoin
* distributed DNS

How Bitcoin Mining Works?

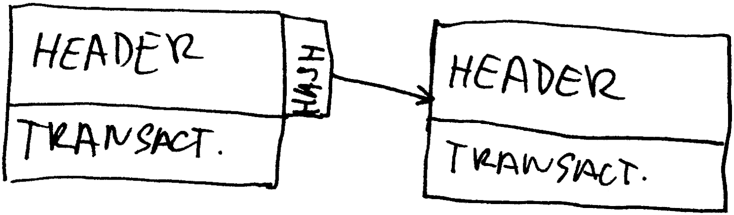
Block

* header
* transactions

Block Header

* version
* hashPrevBlock
* hashMerkelRoot
* time
* bits (difficulty)
* nonce

Blockchain



Mining

Proof of Work

”A proof of work is a piece of data which was difficult (costly, time-consuming) to produce so as to satisfy certain requirements”

```
"Hello, world!0" => 1312af178c253f84...
"Hello, world!1" => e9afc424b79e4f6a...
"Hello, world!2" => ae37343a357a8297...
.
.
.
"Hello, world!4248" => 6e110d98b388e...
"Hello, world!4249" => c004190b822f1...
"Hello, world!4250" => 0000c3af42fc3...
```

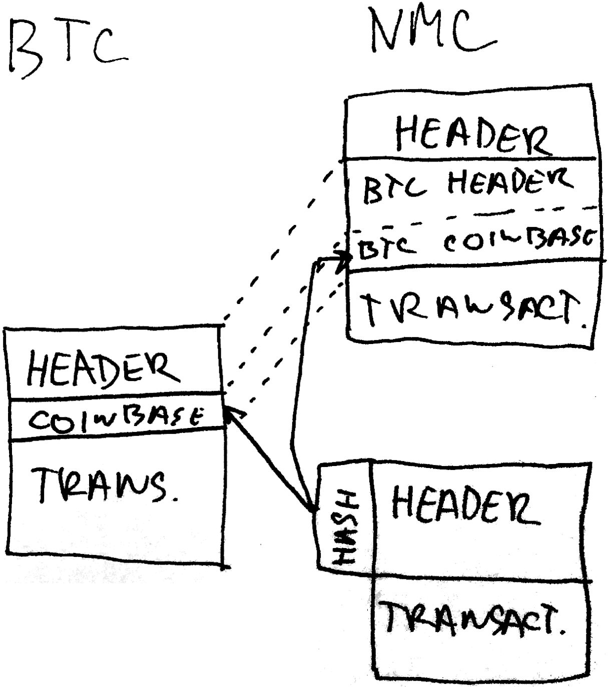
Auxiliary POW

”This is the way that merged mining can exist; it is the relationship between two blockchains for one to trust the other’s work as their own and accept AuxPOW blocks.”

Bitcoin Coinbase

* block height
* flags
* merged mining prefix
* namecoin prevhash
* ...

Principle of Aux POW


BTC
NMC
HEADER
BTC HEADER
BTC COINBASE
TRANSACT.
HEADER
COINBASE
TRANS.
HASH
HEADER
TRANSACT.

Namecoin Block

* header
* auxpow (btc coinbase tx, btc branch, btc header)
* transactions

Thanks & Questions

ondrej@ondrejsika.com
http://ondrejsika.com
@ondrejsika

Sources:
http://url.os1.cz/merged-mining-ctjb/