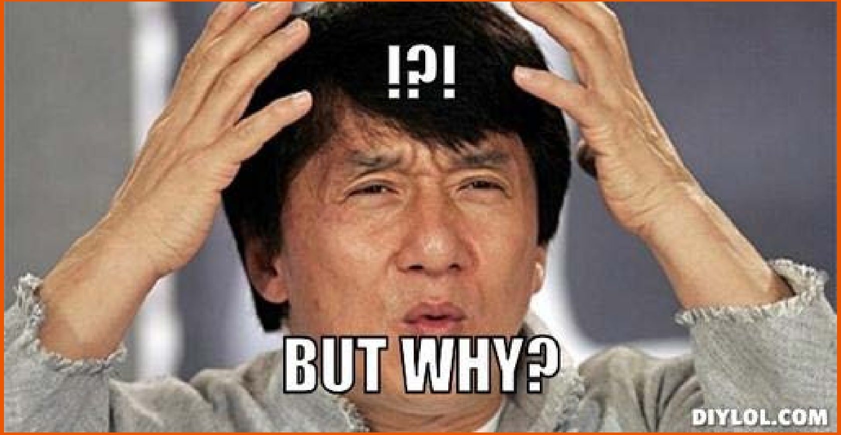
Consensus Mechanisms

By Peter Van Valkenburgh
Director of Research at Coin Center

COIN CENTER

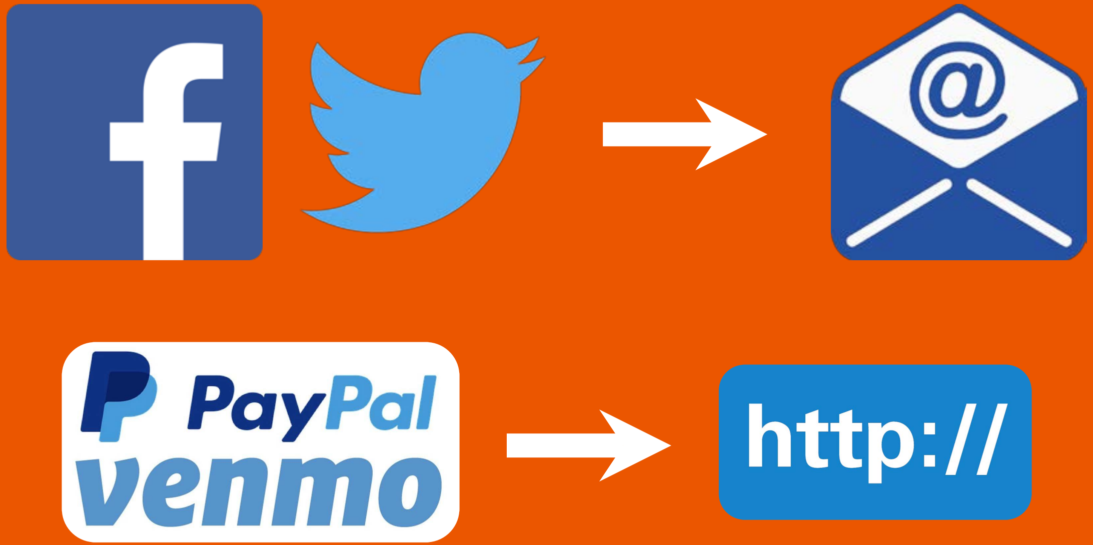
Why Crypto?



Goal:

Take centralized service providers and turn their services into peer-to-peer internet protocols (aka decentralized apps).

Goal:

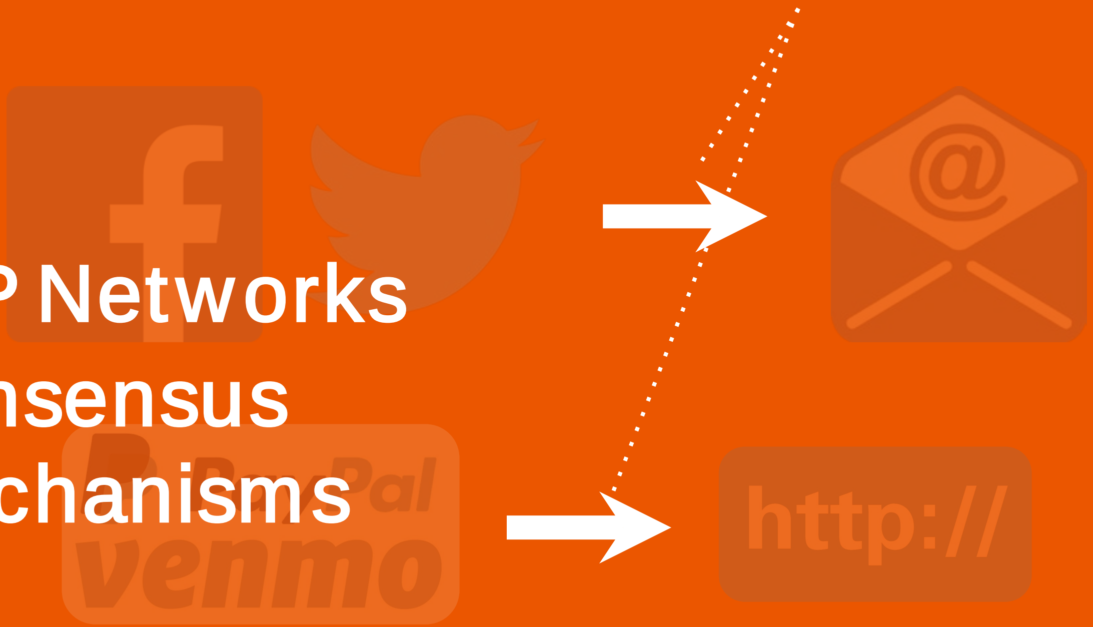


Goal:

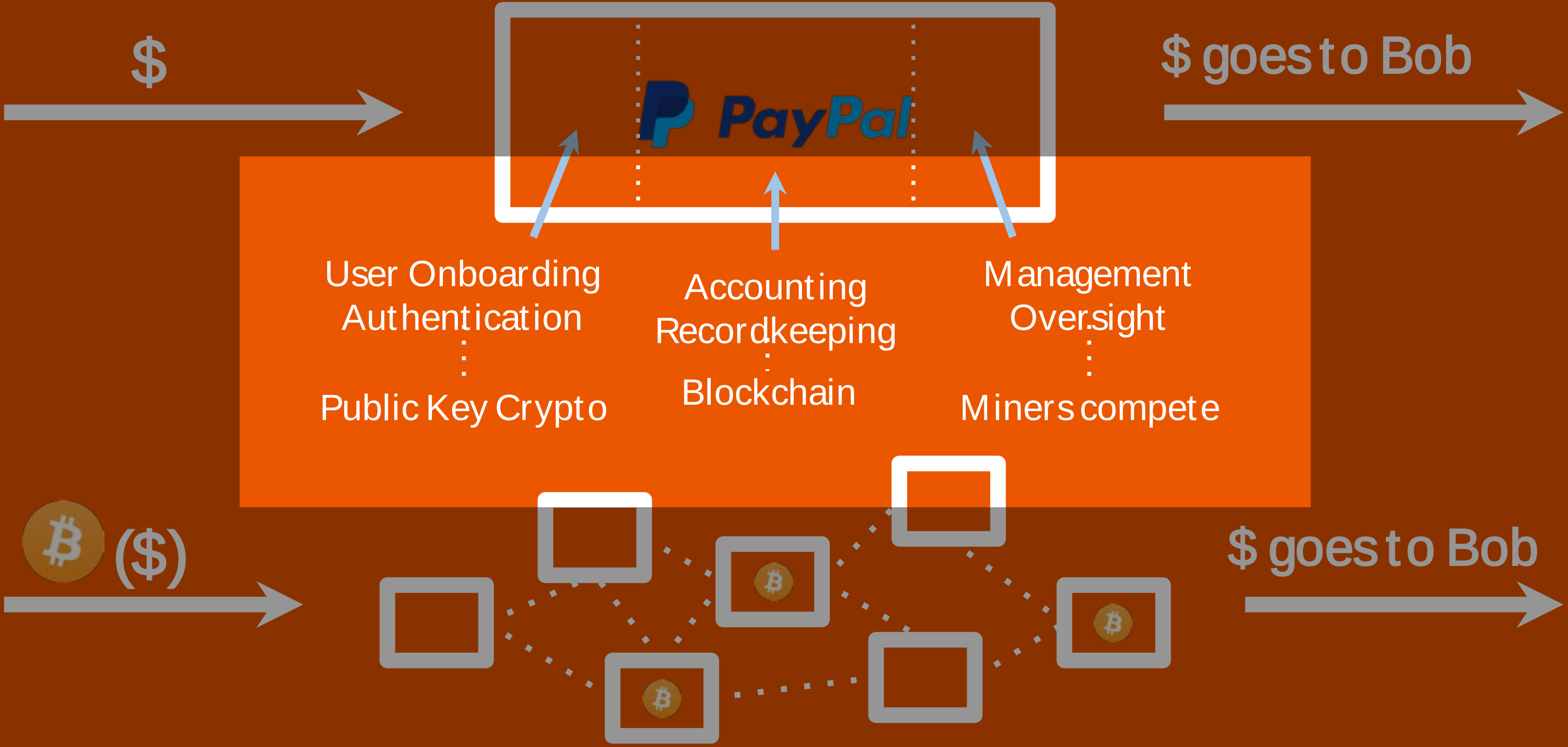
blockchain-crypto-magic®

AKA:

1. P2P Networks
2. Consensus Mechanisms



Decentralized App: Money

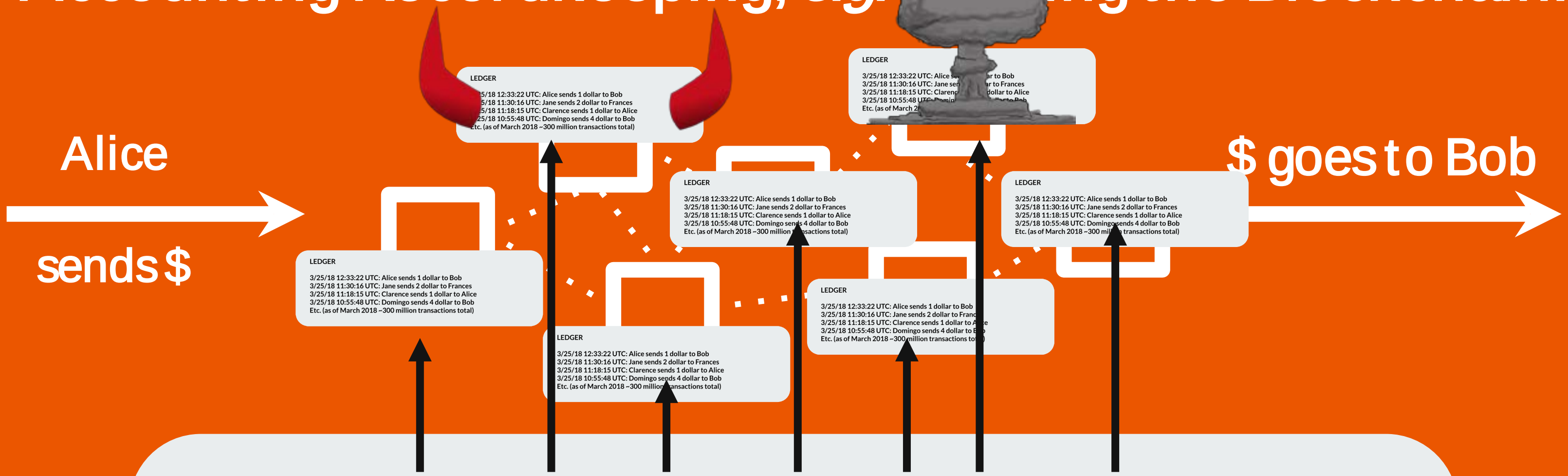


User Onboarding
Authentication
⋮
Public Key Crypto

Accounting
Recordkeeping
⋮
Blockchain

Management
Oversight
⋮
Miners compete

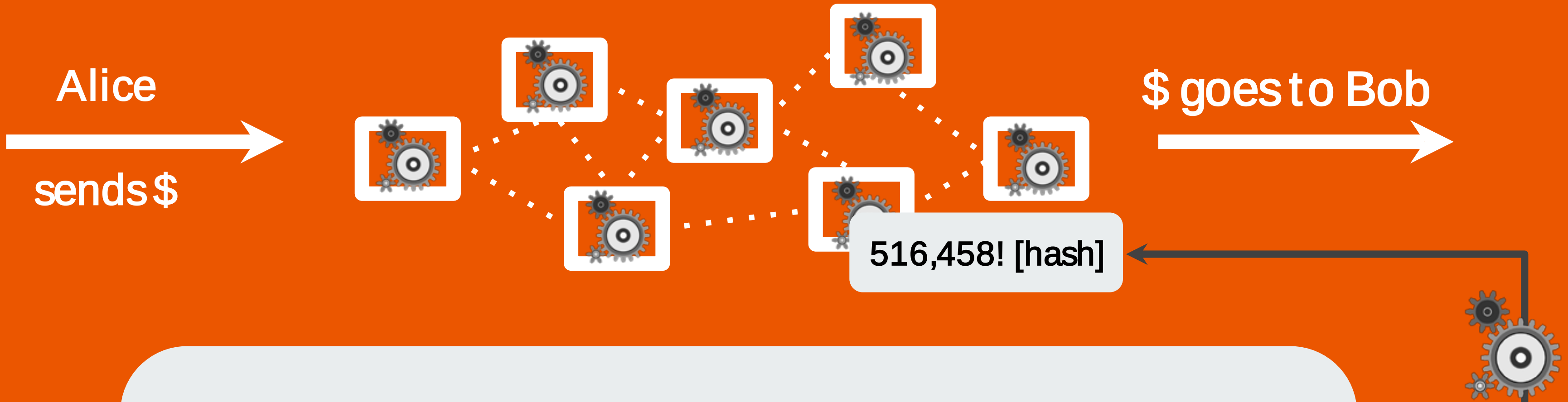
Accounting Recordkeeping, *e.g.* Keeping the Blockchain.


Alice
sends $
$ goes to Bob
LEDGER
5/18 12:33:22 UTC: Alice sends 1 dollar to Bob
5/18 11:30:16 UTC: Jane sends 2 dollar to Frances
5/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
5/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice s ar to Bob
3/25/18 11:30:16 UTC: Jane sen ar to Frances
3/25/18 11:18:15 UTC: Clarenc dollar to Alice
3/25/18 10:55:48 UTC
Etc. (as of March 2
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)
LEDGER
3/25/18 12:33:22 UTC: Alice sends 1 dollar to Bob
3/25/18 11:30:16 UTC: Jane sends 2 dollar to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 dollar to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 dollar to Bob
Etc. (as of March 2018 ~300 million transactions total)

LEDGER

3/25/18 12:33:22 UTC: Alice sends 1 bitcoin to Bob
3/25/18 11:30:16 UTC: Jane sends 2 bitcoin to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 bitcoin to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 bitcoin to Bob
Etc. (as of March 2018 ~300 million transactions total)

Accounting Recordkeeping, *e.g.* Keeping the Blockchain.



Alice

sends $

$ goes to Bob

516,458! [hash]

Block 516
Hash of 5:
Uri sends
Vitalik sei
Dodger se
Josh send
Jerry senc

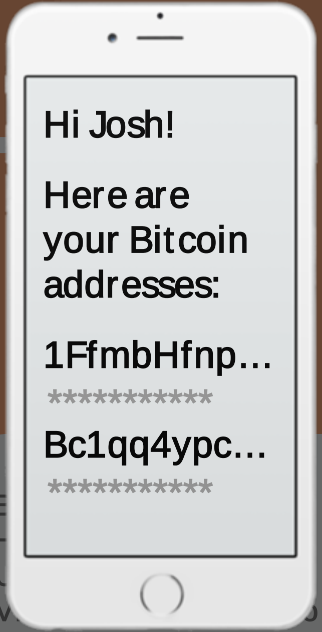
LEDGER

3/25/18 12:33:22 UTC: Alice sends 1 bitcoin to Bob
3/25/18 11:30:16 UTC: Jane sends 2 bitcoin to Frances
3/25/18 11:18:15 UTC: Clarence sends 1 bitcoin to Alice
3/25/18 10:55:48 UTC: Domingo sends 4 bitcoin to Bob
Etc. (as of March 2018 ~300 million transactions total)

es
ice
ob
ary

MEGA MILLIONS featuring MEGAPLIER
MEGA 09 QP
A. 08 17 55 58 62 QP
MEGAPLIER OPTION NO
TUE NOV04 14
WISCONSIN'S MEGA BUCKS
A. 05 17 24 37 41 49 QP
B. 01 04 05 18 26 31 QP
C. 02 05 12 13 30 39 QP
D. 02 07 27 30 41 45 QP
POWERBALL POWERPLAY
A. 11 17 21 26 38 QP POWER 06 QP
B. 09 20 23 28 47 QP 35 QP
C. 13 15 24 25 43 QP 08 QP
D. 24 25 26 32 46 QP 30 QP
POWER PLAY OPTION NO $8.00
WED JUN11 14
A. 11 34 35 41 58 QP POWER 10 QP
POWER PLAY OPTION NO
WED JUL09 14
$2.00
A. 02 16 22 24
B. 04 20 43 44
C. 06 32 41 51
POWER PLAY
WED DEC
A. 06 09 19 20 21 QP
B. 08 12 13 14 20 QP
POWER PLAY OPTION
SAT JAN04 14
Wisconsin Lottery

User Onboarding Authentication e.g. Public Key Crypto



Hi Josh!

Here are your Bitcoin addresses:

1FfmbHfnp…
****

Bc1qq4ypc…
****

Block 516,455
Hash of 516,454
1DWLS 3 bitcoin to 1Nvwx….[sig]
14XP2 14 bitcoin to 1al46……[sig]
18gB4 10 bitcoin to 1xtO3…..[sig]
1Ffmb 8 bitcoin to 1Favyr…….[sig]
1S4mX 6 bitcoin to 1x8zU……[sig]

Hi Antonie!

Here are your Bitcoin addresses:

1FavyrdAw…
****

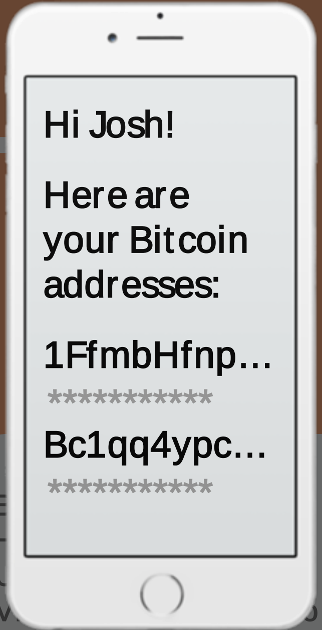
Generate New?

E
H
U
V o Vlad
Dodger sends 10 dollar to Zooko
Josh sends 8 dollar to Antonie
Jerry sends 6 dollar to Neeraj

Hadeel sends 3 dollar to Yoon
Tracey sends 12 dollar to Sibille
Petras sends 2 dollar to Ingrid
Sedat sends 6 dollar to Paula

6,4
516
ends
Jane sends 2
Clarence sends 1 dollar to Alice
Domingo sends 4 dollar to Bob
Charley sends 12 dollar to Mary

User Onboarding Authentication e.g. Public Key Crypto



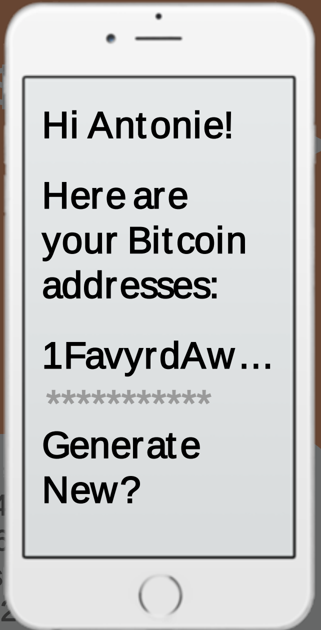
Hi Josh!

Here are your Bitcoin addresses:

1FfmbHfnp…
****

Bc1qq4ypc…
****

Block 516,455
Hash of 516,454
1DWLS 3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr........[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]



Hi Antonie!

Here are your Bitcoin addresses:

1FavyrdAw…
****

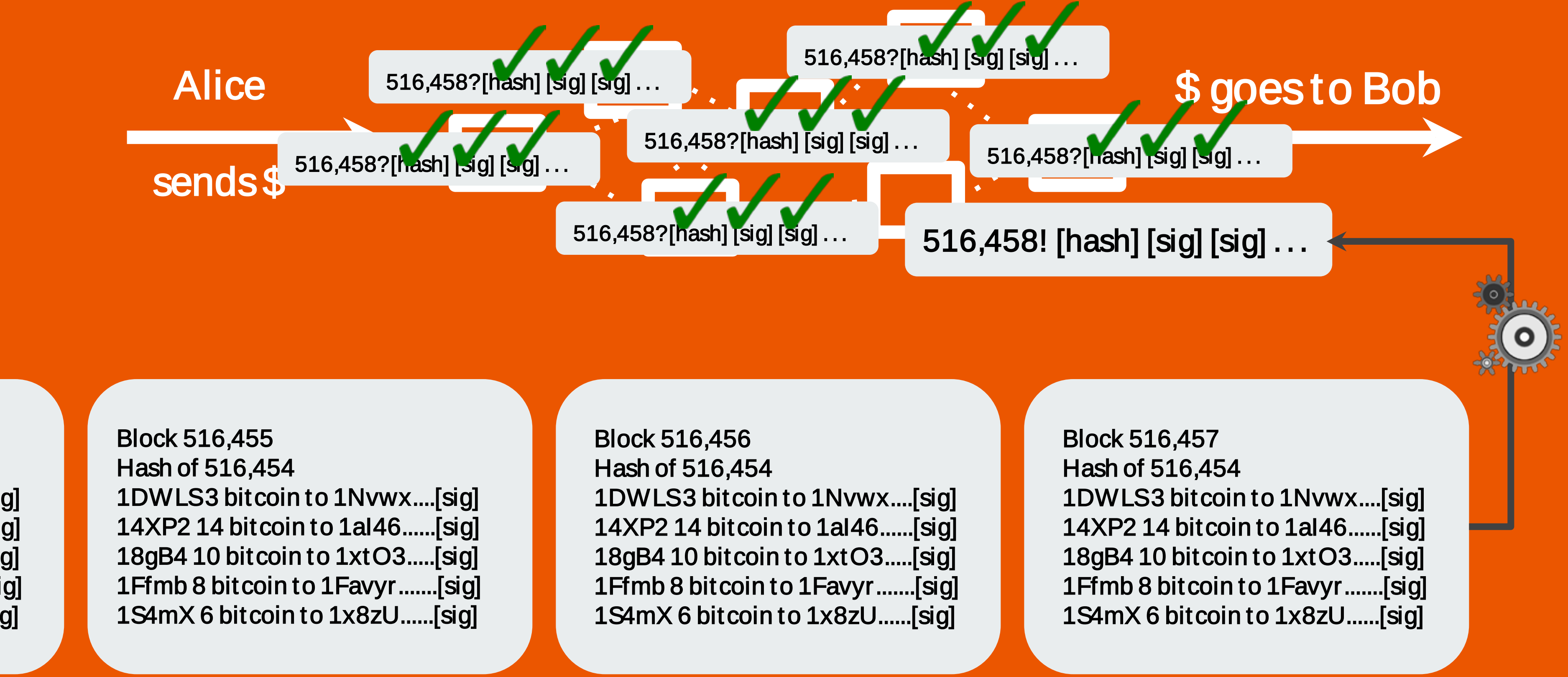
Generate New?

o Vlad
Dodger sends 10 dollar to Zooko
Josh sends 8 dollar to Antonie
Jerry sends 6 dollar to Neeraj

Hadeel sends 3 dollar to Yoon
Tracey sends 12 dollar to Sibille
Petras sends 2 dollar to Ingrid
Sedat sends 6 dollar to Paula

6,4
516
ends
Jane sends 2
Clarence sends 1 dollar to Alice
Domingo sends 4 dollar to Bob
Charley sends 12 dollar to Mary

User Onboarding Authentication e.g. Public Key Crypto



Alice

sends $

516,458?[hash] [sig] [sig] . . .

516,458?[hash] [sig] [sig] . . .

516,458?[hash] [sig] [sig] . . .

516,458?[hash] [sig] [sig] . . .

516,458?[hash] [sig] [sig] . . .

516,458?[hash] [sig] [sig] . . .

$ goes to Bob

516,458! [hash] [sig] [sig] . . .

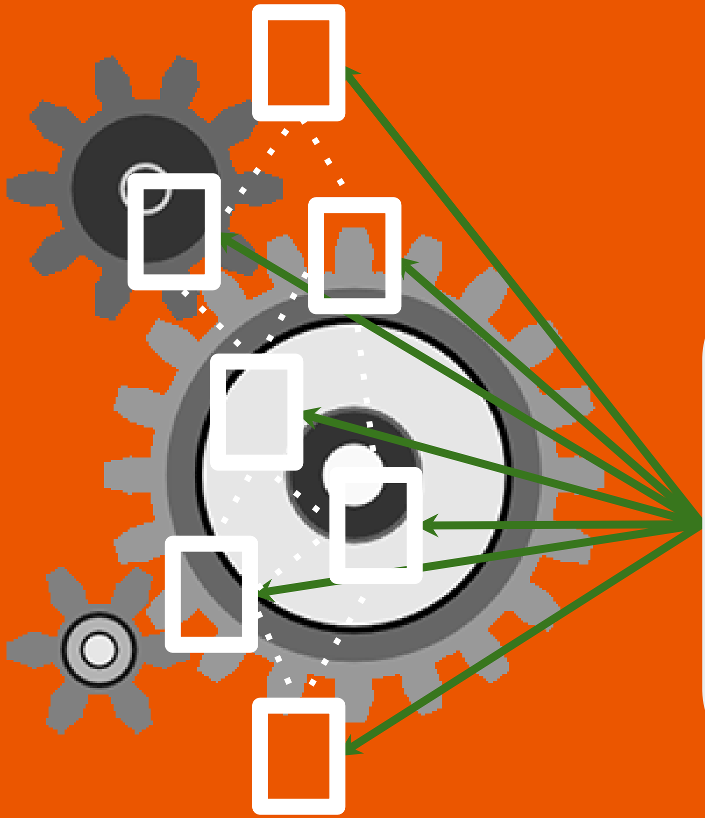
g]
g]
g]
ig]
g]

Block 516,455
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Why do all the work?

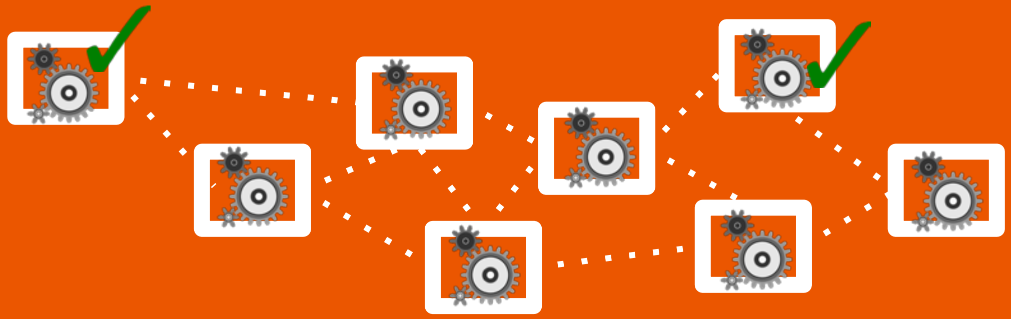


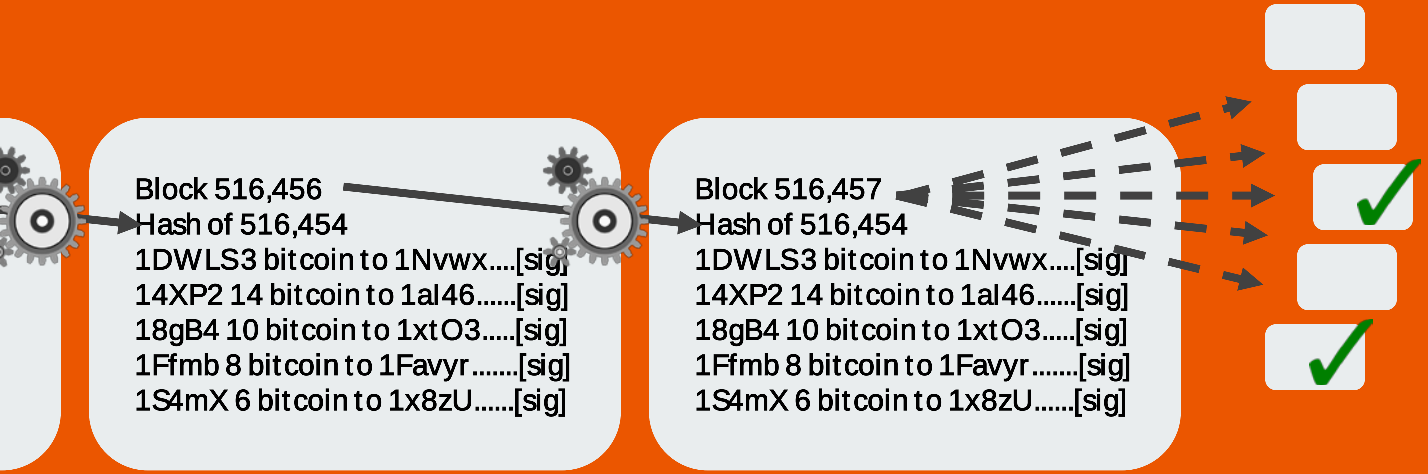
Block 516,458
Hash of 516,457 ✓

1DWLS… 3 bitcoin to 1Nvwx…[sig] ✓ [fee goes to miner]
14XP2… 14 bitcoin to 1al46…[sig] ✓ [fee goes to miner]
18gB4… 10 bitcoin to 1xtO3…[sig] ✓ [fee goes to miner]
1Ffmb… 8 bitcoin to 1Favyr…[sig] ✓ [fee goes to miner]

12.5 bitcoin to ✓ 1x8zU (miner's address)

Proof of Work Consensus Mechanisms are Open

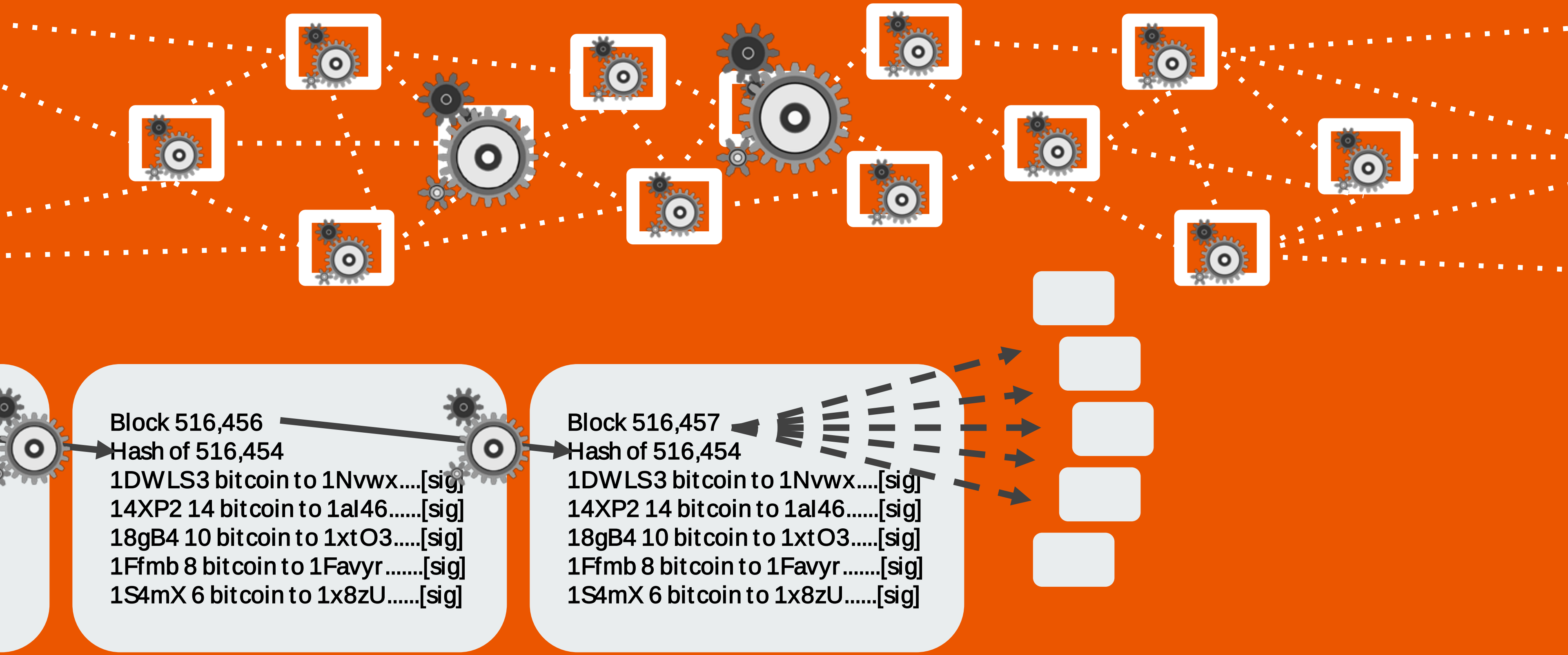




Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

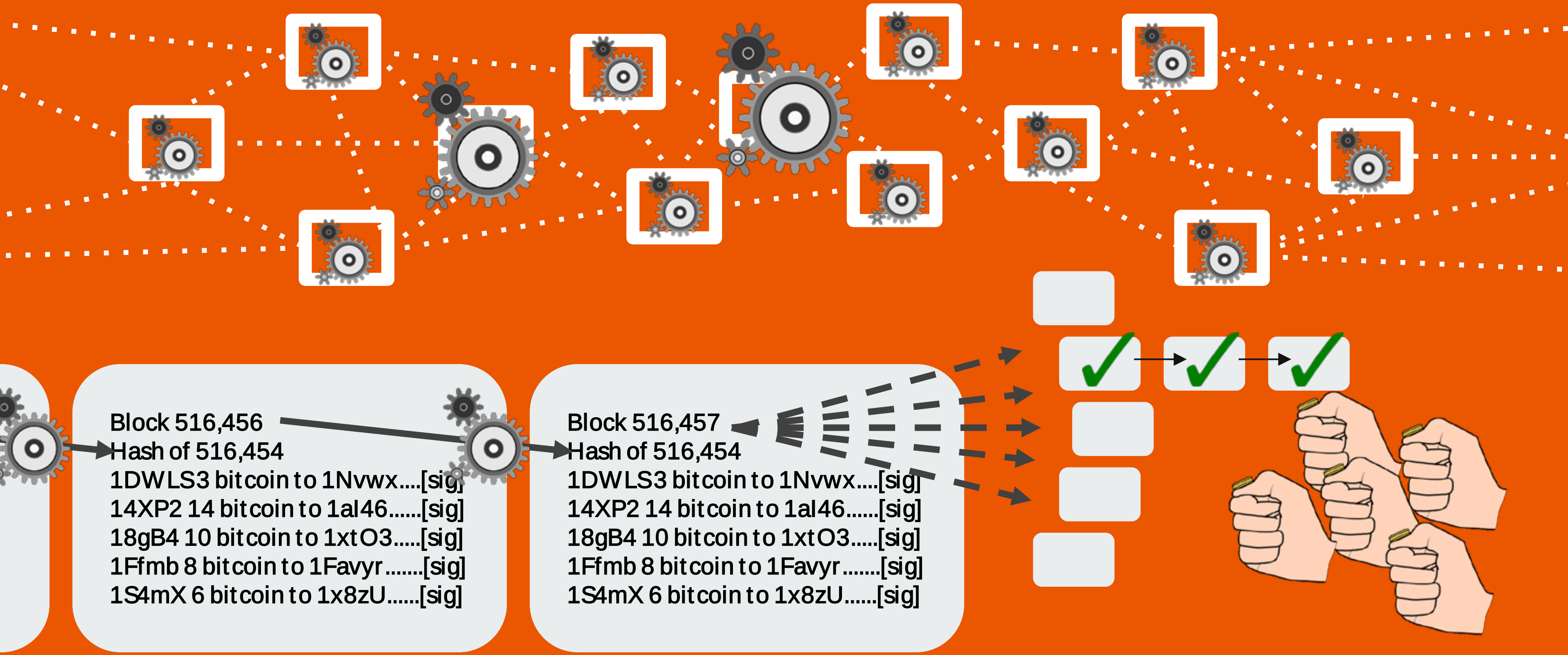
Proof of Work Consensus Mechanisms are Open



Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

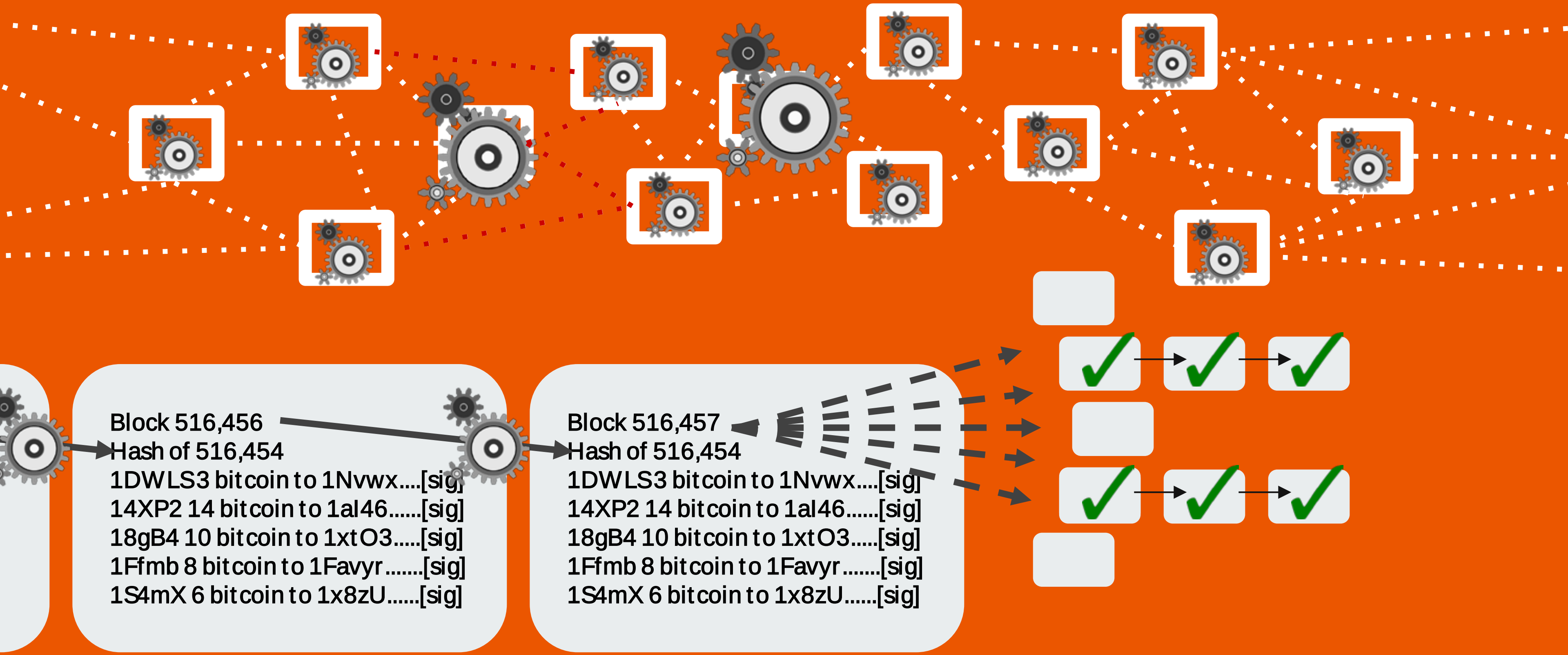
Proof of Work Consensus has Adjustable Difficulty



Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

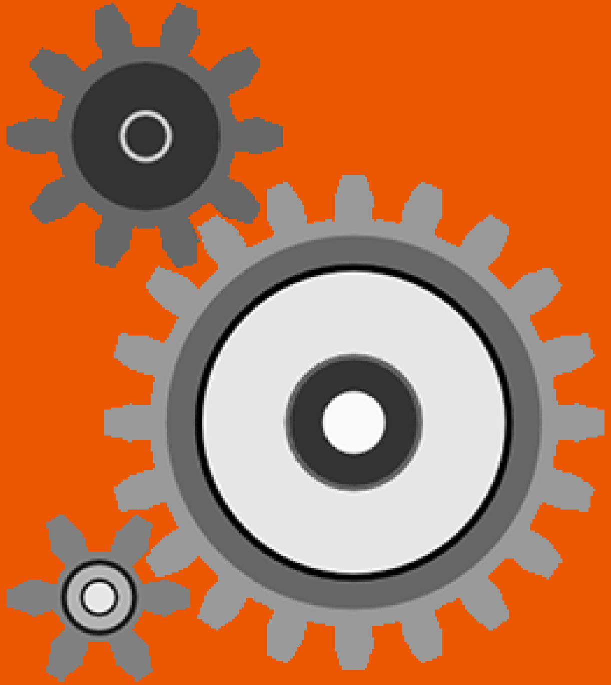
Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Proof of Work Consensus has Adjustable Difficulty



Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1aI46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1aI46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

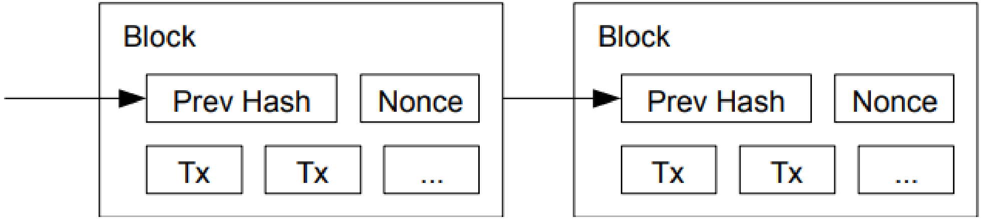


If blocks have been coming around faster on average, the difficulty increases and vice versa.

Mining Hardware and “ASIC Resistance”

MEGA MILLIONS
featuring MEGAPLIER
MEGA 09 QP
A. 08 17 55 58 62 QP
MEGAPLIER OPTION NO $1
TUE NOV04 14
19379700 439-4360475
WISCONSIN'S MEGA BUCKS
A. 05 17 24 37 41 49 QP
B. 01 04 05 18 26 31 QP
C. 02 05 12 13 30 39 QP
D. 02 07 27 30 41 45 QP
POWERBALL
POWERPLAY
POWER
A. 11 17 21 26 38 QP 06 QP
B. 09 20 23 28 47 QP 35 QP
C. 13 15 24 25 43 QP 08 QP
D. 24 25 26 32 46 QP 30 QP
POWER PLAY OPTION NO $8.00
WED JUN11 14
292-2451 2007-120607
A. 11 34 35 41 58 QP POWER 10 QP
POWER PLAY OPTION NO
WED JUL09 14
$2.00
013885 18285700
A. 02 16 22 24
B. 04 20 43 44
C. 06 32 41 51
POWER PLAY
WED DEC
A. 06 09 19 20 21 QP
B. 08 12 13 14 20 QP
POWER PLAY OPTION
SAT JAN04 14
133-57882112-1
07 24 34
02 16 30
POWER PLAY
WED NOV
POWER 23 QP
56 QP 23 QP
3 57 QP
Wisconsin Lottery

without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



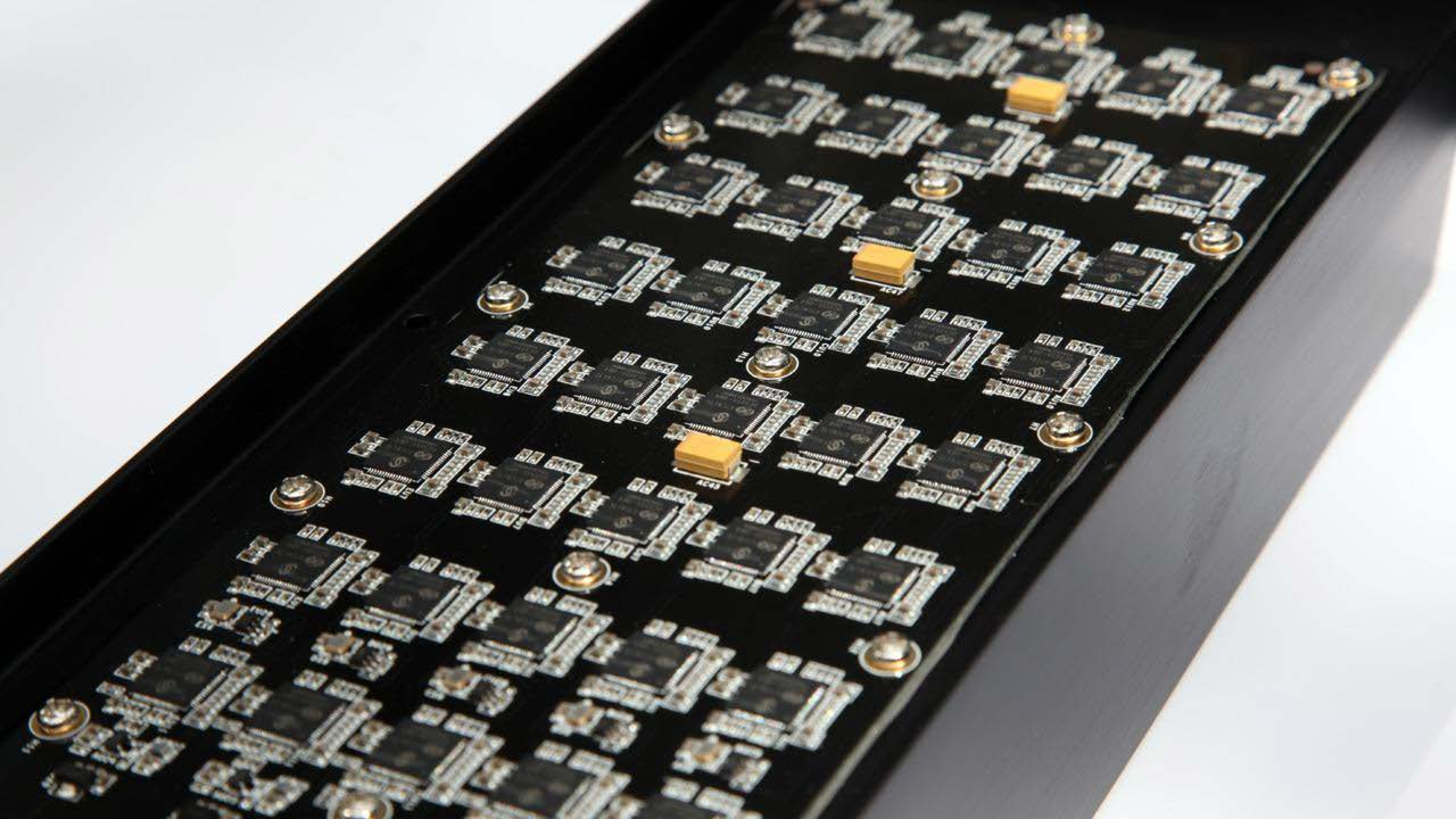
The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5 Network

```
nikhil@nikhil-desktop-ubuntu: ~
Preparing to unpack .../011-libxres1_2%3a1.0.7-1_amd64.deb ...
Unpacking libxres1:amd64 (2:1.0.7-1) over (2:1.0.7-1) ...
Preparing to unpack .../012-libwnck-3-common_3.24.1-1_all.deb ...
Unpacking libwnck-3-common (3.24.1-1) over (3.20.1-1) ...
Preparing to unpack .../013-libwnck-3-0_3.24.1-1_amd64.deb ...
Unpacking libwnck-3-0:amd64 (3.24.1-1) over (3.20.1-1) ...
Preparing to unpack .../014-session-migration_0.3.2_amd64.deb ...
Unpacking session-migration (0.3.2) over (0.3) ...
Preparing to unpack .../015-libgcab-1.0-0_0.7-4_amd64.deb ...
Unpacking libgcab-1.0-0:amd64 (0.7-4) over (0.7-2) ...
Preparing to unpack .../016-libappstream-glib8_0.7.1-2_amd64.deb ...
Unpacking libappstream-glib8:amd64 (0.7.1-2) over (0.6.9-1) ...
Preparing to unpack .../017-compiz_1%3a0.9.13.1+17.10.20170901-0ubuntu1_all.deb ...
Unpacking compiz (1:0.9.13.1+17.10.20170901-0ubuntu1) over (1:0.9.13.1+17.04.20170109-0ubuntu1) ...
Preparing to unpack .../018-nux-tools_4.0.8+17.10.20170922-0ubuntu1_amd64.deb ...
Unpacking nux-tools (4.0.8+17.10.20170922-0ubuntu1) over (4.0.8+17.04.20170213-0ubuntu1) ...
Preparing to unpack .../019-unity-asset-pool_0.8.24+17.10.20170507-0ubuntu1_all.deb ...
Unpacking unity-asset-pool (0.8.24+17.10.20170507-0ubuntu1) over (0.8.24+15.04.20141217-0ubuntu2) ...
Preparing to unpack .../020-unity-greeter_17.10.0-0ubuntu1_amd64.deb ...
Unpacking unity-greeter (17.10.0-0ubuntu1) over (17.04.0-0ubuntu1) ...
Preparing to unpack .../021-unity-scopes-master-default_6.0.2+16.04.20160212.1-0ubuntu2_all.deb ...
Unpacking unity-scopes-master-default (6.0.2+16.04.20160212.1-0ubuntu2) over (6.0.2+16.04.20160212.1-0ubuntu1) ...
Preparing to unpack .../022-unity-scope-home_6.0.2+16.04.20160212.1-0ubuntu2_amd64.deb ...
Unpacking unity-scope-home (6.0.2+16.04.20160212.1-0ubuntu2) over (6.0.2+16.04.20160212.1-0ubuntu1) ...
Selecting previously unselected package unity-session.
Preparing to unpack .../023-unity-session_3.26.1-0ubuntu0_all.deb ...
Unpacking unity-session (3.26.1-0ubuntu0) ...
Preparing to unpack .../024-libmenu-cache-bin_1.0.2-3ubuntu0.17.10.1_amd64.deb ...
Unpacking libmenu-cache-bin (1.0.2-3ubuntu0.17.10.1) over (1.0.2-1ubuntu0.1) ...
Preparing to unpack .../025-libmenu-cache3_1.0.2-3ubuntu0.17.10.1_amd64.deb ...
Unpacking libmenu-cache3:amd64 (1.0.2-3ubuntu0.17.10.1) over (1.0.2-1ubuntu0.1) ...
Selecting previously unselected package openbox-menu.
Preparing to unpack .../026-openbox-menu_0.8.0+hg20161009-1_amd64.deb ...
Unpacking openbox-menu (0.8.0+hg20161009-1) ...
Preparing to unpack .../027-libobt2v5_3.6.1-5_amd64.deb ...
Unpacking libobt2v5 (3.6.1-5) over (3.6.1-4ubuntu1) ...
Preparing to unpack .../028-libobrender32v5_3.6.1-5_amd64.deb ...
Unpacking libobrender32v5 (3.6.1-5) over (3.6.1-4ubuntu1) ...
Preparing to unpack .../029-openbox_3.6.1-5_amd64.deb ...
Unpacking openbox (3.6.1-5) over (3.6.1-4ubuntu1) ...
Preparing to unpack .../030-wmaker-common_0.95.8-2_all.deb ...
Unpacking wmaker-common (0.95.8-2) over (0.95.7-8) ...
```

COIN CENTER
1255



51% Attacks?

Still not a major threat to cryptocurrencies with competitive mining because of the tremendous costs involved.

Real threat to poorly-capitalized cryptocurrencies that share a mining algorithm with a larger cryptocurrency.

ethereum

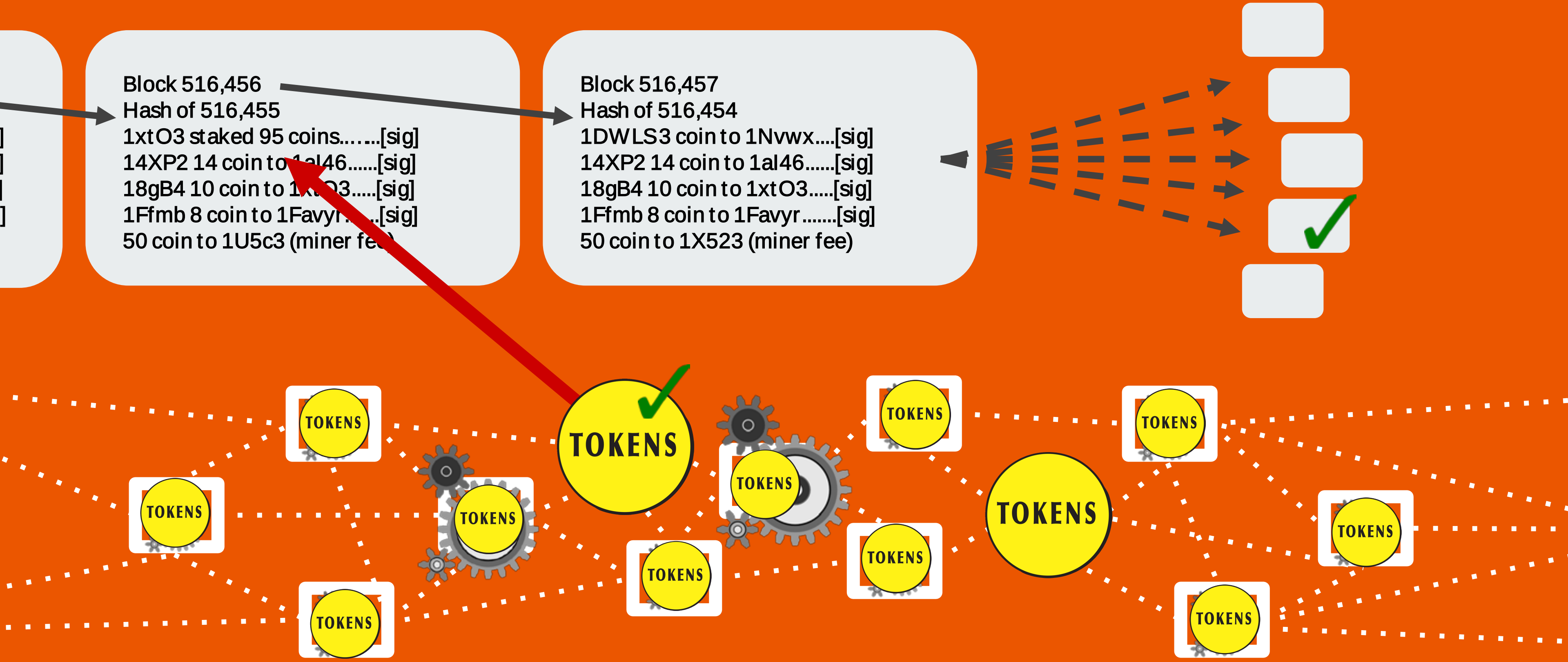
ethereum
classic

Proof of Stake

MEGA MILLIONS
featuring MEGAPLIER
WISCONSIN'S MEGA BUCKS
POWERBALL
POWERPLAY
Wisconsin Lottery

How do you get a lottery ticket in order to have a chance to participate?

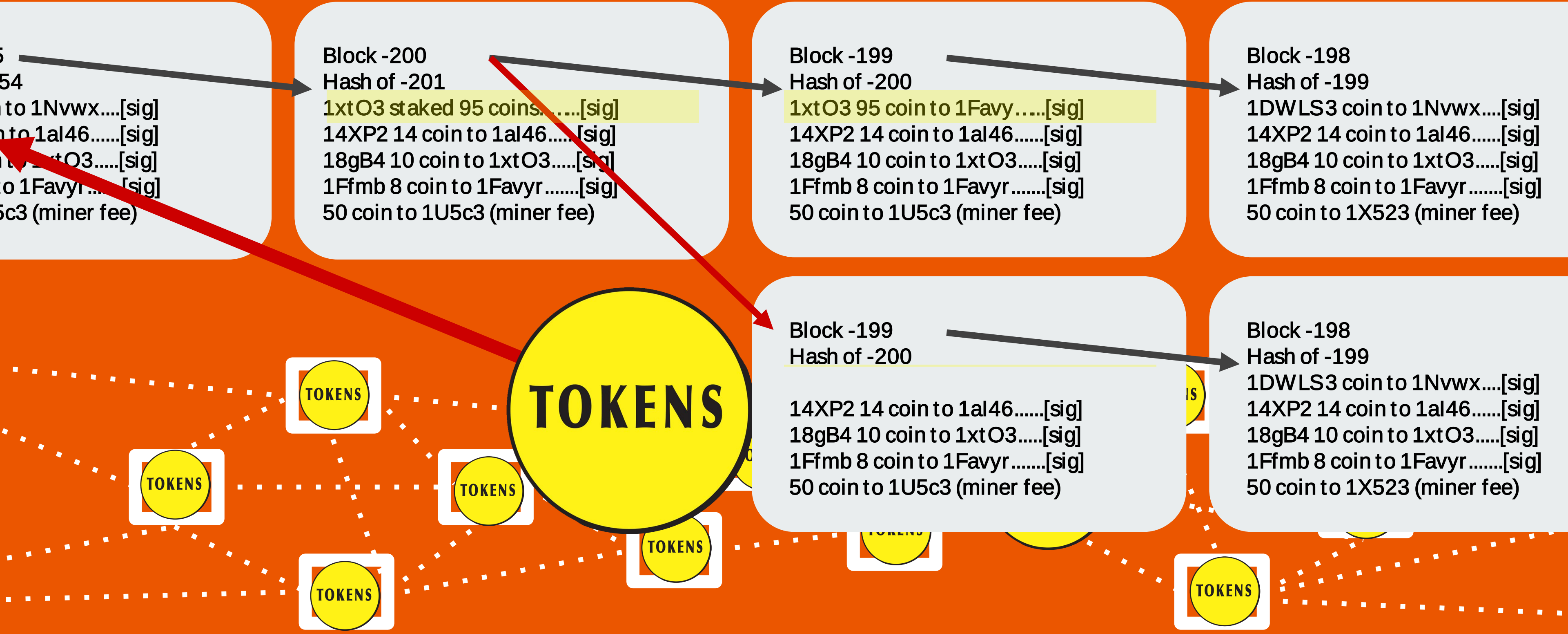
Proof of Stake: How do you get a ticket?



Block 516,456
Hash of 516,455
1xtO3 staked 95 coins.........[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block 516,457
Hash of 516,454
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

Proof of Stake: Nothing at Stake?



5
54
n to 1Nvwx....[sig]
n to 1al46......[sig]
n to 1xtO3.....[sig]
o 1Favyr.......[sig]
5c3 (miner fee)

Block -200
Hash of -201
1xtO3 staked 95 coins........[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block -199
Hash of -200
1xtO3 95 coin to 1Favy........[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block -198
Hash of -199
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

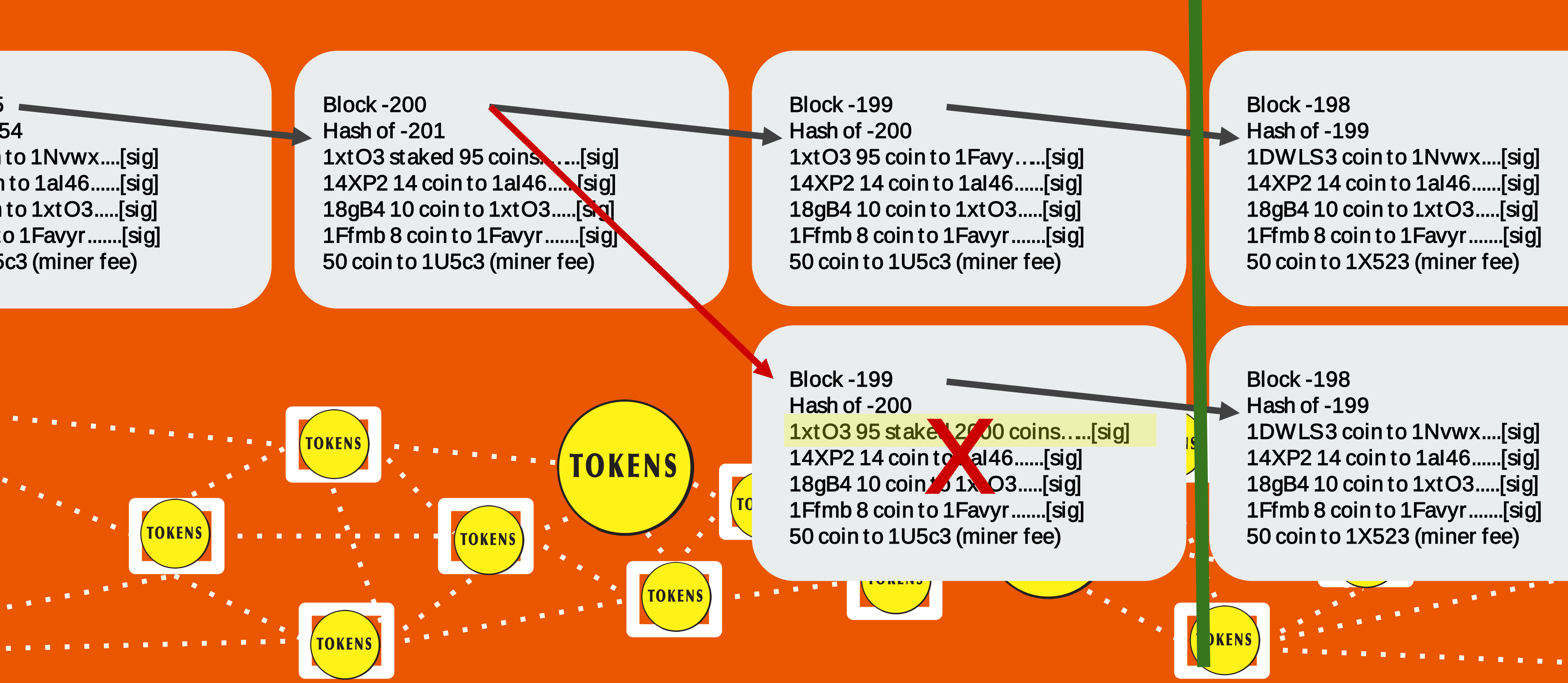
Block -199
Hash of -200

14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block -198
Hash of -199
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

peercoin

Proof of Stake: Checkpoints to stop “nothing at stake”



5
54
n to 1Nvwx....[sig]
n to 1al46......[sig]
n to 1xtO3.....[sig]
o 1Favyr.......[sig]
5c3 (miner fee)

Block -200
Hash of -201
1xtO3 staked 95 coins…...[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block -199
Hash of -200
1xtO3 95 coin to 1Favy…...[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block -198
Hash of -199
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

Block -199
Hash of -200
1xtO3 95 staked 2000 coins…...[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

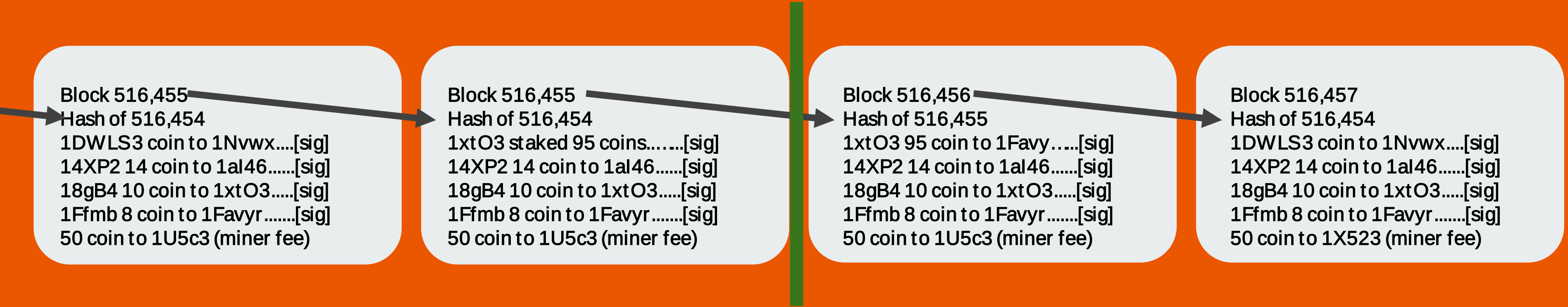
Block -198
Hash of -199
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

But who does the checkpointing?

peercoin

Or some subset of stakers?
E.g. 2/3 of validators in Ethereum’s Casper Protocol

Finality in PoS vs PoW



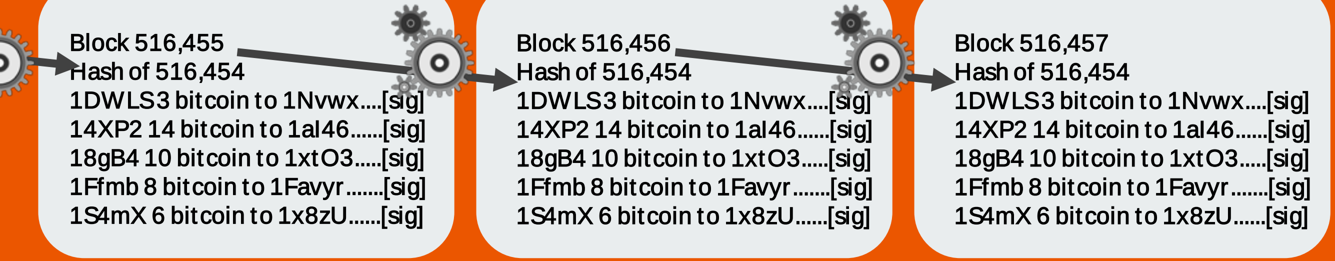
Block 516,455
Hash of 516,454
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block 516,455
Hash of 516,454
1xtO3 staked 95 coins…....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block 516,456
Hash of 516,455
1xtO3 95 coin to 1Favy…..[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1U5c3 (miner fee)

Block 516,457
Hash of 516,454
1DWLS3 coin to 1Nvwx....[sig]
14XP2 14 coin to 1al46......[sig]
18gB4 10 coin to 1xtO3.....[sig]
1Ffmb 8 coin to 1Favyr.......[sig]
50 coin to 1X523 (miner fee)

Proof of stake: wait until transaction is in a block prior to an accepted checkpoint.



Block 516,455
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,456
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Block 516,457
Hash of 516,454
1DWLS3 bitcoin to 1Nvwx....[sig]
14XP2 14 bitcoin to 1al46......[sig]
18gB4 10 bitcoin to 1xtO3.....[sig]
1Ffmb 8 bitcoin to 1Favyr.......[sig]
1S4mX 6 bitcoin to 1x8zU......[sig]

Proof of work: wait until transaction is in a block old enough that computing effort to recreate chain since is cost-prohibitive.

Forks?

- Consensus mechanisms are designed to prevent forks among participants who WANT to stay together.
  - Forks and reorganizations can happen but they should be short-lived and only involve a small number of blocks.

- If a group within the community fundamentally disagrees with the rest and no longer wish to stay together, then they may fork by breaking compatibility, i.e. altering the consensus rules that they follow.
  - Forks will be long-lived but two distinct assets will result.

Implications for Traders and Funds

- PoS vs. Pow?
  - Generally not relevant —just another way of building a provably fair lottery for block creation.
  - May impact best practices for finality.
    PoS: Checkpointing vs. PoW: Computational Infeasibility
  - Take-away: Institutional participants should have documented procedures for how risks around finality will be mitigated.

Implications for Traders and Funds

- 51% Attacks?
  - Not a major risk for well-capitalized cryptos.
  - Major risk for poorly-capitalized cryptos that share common mining algo with larger crypto.
  - Takeaway: Institutional participants should be wary of poorly-capitalized cryptos that share a mining algo with larger cryptos.

Implications for Traders and Funds

- Forks?
  - Well-specified PoW and PoS systems may have occasional unintentional forks but they will not persist or involve deep block reorganizations.
  - Takeaway: Have prudent and well-documented procedures over finality; procedures to pause trading during forks.

Implications for Traders and Funds

- Forks?
    - When a subset of community members reach intractable disagreements with the rest of the community, they may choose to alter the consensus rules and permanently fork.
    - Takeaway: Institutional participants should have well-documented procedures describing how they will determine which fork to honor, and what to do with any windfalls from the other fork.

Questions?

Peter Van Valkenburgh
peter@coincenter.org
@valkenburgh

COIN CENTER