The Role of Cryptography in Distributed Systems

Roger Wattenhofer
Disclaimer

(No ECC, not even Crypto.)
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis.
Blockchain Basics
Transaction
Block
Blockchain is Replicated
Fundamental Problem: Byzantine Agreement (Consensus)
3 nodes

[Lamport, Shostak, Pease, 1982]
Byzantine Agreement
Impossible with 1/3 Baddies...
... unless we use Crypto!
3 nodes, signatures
But Without Crypto?!
Voting Framework

vote = input
send vote to all
wait for n-f votes

all
0
+3f
vote
0
1
+3f
(n-f/2)
+3f
all
1
decide
0
decide
1
vote
0
vote
1
Voting Framework

all

0

decide

vote

0

0

vote

1

1

+3f

+f

(n-f)/2

+f

+3f

→

all

1
\[
\frac{(n-f)}{2}
\]
\((n-f)/2\)
Boundary between Crypto and No Crypto?
Encrypted Bitstring
Encrypted Bitstring
Overview
Challenge: Fast Byzantine Agreement Without Crypto
Detecting Byzantine nodes

\[ \times n^2 \]

sum of all +/- coinflips
Detecting Byzantine nodes

\[ n^2 \times \text{sum of all +/- coinflips} \]

Total sum has to be close to 0
## Detecting Byzantine nodes

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

[King & Saia, 2016]
Detecting Byzantine nodes
Detecting Byzantine nodes

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Or Rather...?
crypto? no

[King & Saia, 2016]

[Ben-Or, 1983]

[Melnyk, Wang, W, Draft only]
Fast Byzantine Agreement
Without Crypto Still Open!
What is the Power of Crypto?
What is Crypto?
Thank You!
Questions & Comments?

Thanks to my co-authors
Darya Melnyk, Yuyi Wang

www.disco.ethz.ch