Bitcoin’s Technical Challenges

Christian Decker
Bitcoin Basics
Bitcoin Basics
## Bitcoin Basics

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
Bitcoin Basics

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24</td>
</tr>
<tr>
<td>B</td>
<td>53</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>

A TX is depicted, suggesting a transaction or transfer process.
Transferring Bitcoins

TX: 41b221
Transferring Bitcoins

TX: 41b221

Inputs

Outputs

<table>
<thead>
<tr>
<th>Outputs</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.001</td>
</tr>
</tbody>
</table>


Transferring Bitcoins

TX: 41b221

A → 4.899
TX: 41b221

0.1

B

A

4.798
Transferring Bitcoins

Inputs

A → 4.899

TX: 41b221

Outputs

B

0 0.1

A

1 4.798

0
Transferring Bitcoins

Inputs

A

4.899

TX: 41b221

Fee

0.001

Outputs

0

B

0.1

A

4.798

1
Transferring Bitcoins

Prev. TX: a1a53743

Outputs | Inputs
---|---
0 | 4.899
... | 4.899
1 | 4.899

TX: 41b221

Fee: 0.001

Outputs:

0 | 0.1
4.798 | 1

B | A
Distributing the Bank
Distributing the Bank
Distributing the Bank
Distributing the Bank
Doublespending
Doublespending

Inputs

$TX$

$TX'$

Outputs
Doublespending
Transaction Conflicts
Transaction Conflicts
Transaction Conflicts
Resolving Conflicts
Resolving Conflicts
How to Choose a Leader?
Securing Fast Payments
Let’s Buy a Snack
Transaction Confidence

\[ \text{TX confidence} (\text{TX}) = \]
Transaction Confidence

\[
\text{confidence}(TX) = \underline{\hspace{2cm}}
\]
Transaction Confidence

\[ \text{confidence}(TX) = \text{value} \]
Transaction Confidence

\[
\text{confidence}(TX) = \text{[Green bar]} \quad \text{[White bar]}
\]
Transaction Confidence

\[
\text{confidence}(TX) = \underline{\text{green bar}}
\]
Successful Doublespend

Probability of successful double spend

Node sample size

Probability

0.088%
Privacy
How (not) to Lose 500 Million USD
Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks.
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack

Red!
Transaction Malleability Attack

Refund

MT.GOX
Incident Timeline

Cumulative malleable doublespends

- 1st Press Release
- 2nd Press Release

386 BTC
Does Bitcoin Scale?
The Bitcoin Ecosystem is Growing
Propagation Speed

http://bitcoinstats.com
Propagation Speed

http://bitcoinstats.com
Propagation Speed

http://bitcoinstats.com
Propagation Speed

http://bitcoinstats.com
Blockchain

Time
Blockchain

Time
Blockchain
Blockchain
Forks

Blockchain forks

Forks

Blockchain Height

1.69%
GHOST
Bitcoin Meets Strong Consistency

TX votes (TX) =
Bitcoin Meets Strong Consistency

TX votes (TX) =
Bitcoin Meets Strong Consistency

votes(TX) =
Bitcoin Meets Strong Consistency

\[
\text{votes}(TX) = \begin{array}{c|c|c|c|c|c}
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c}
\hline
(a,1) & (b,1) & (c,2) & (d,0) & (e,1) & (f,1) \\
\hline
(h,1) & (i,1) & (j,1) \\
\hline
\end{array}
\]
Bitcoin Meets Strong Consistency

\[ votes(TX) = \]
Bitcoin Meets Strong Consistency

\[ \text{votes}(TX) = \]

\[ (a,1) \quad (b,1) \quad (c,2) \quad (d,0) \quad (e,1) \quad (f,1) \quad (g,1) \quad (h,1) \quad (i,1) \quad (j,1) \]
Summary

- Bitcoin is not perfect...
Summary

- Bitcoin is not perfect...
- ...but we’re working on it
Summary

- Bitcoin is not perfect...
- ...but we’re working on it
- Be aware of tradeoffs!
Thank you, questions?