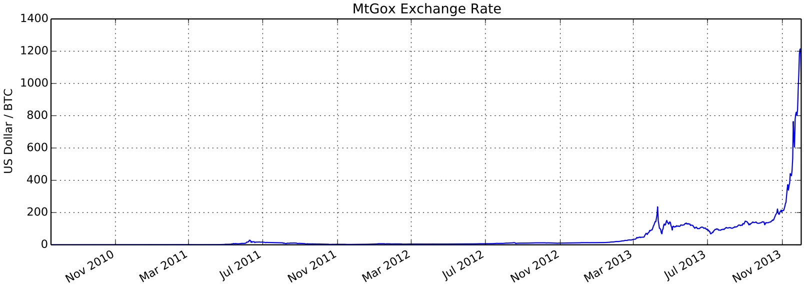
Bitcoin Transaction Malleability and MtGox

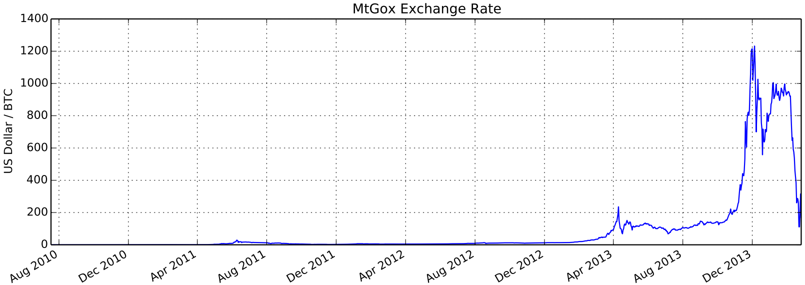
Christian Decker

AEQUITAS
LIBERTAS
VERITAS
21.000.000 AD INFINITUM
2009
IN CRYPTOGRAPHY WE TRUST

Exchanges


MtGox Exchange Rate
US Dollar / BTC
1400
1200
1000
800
600
400
200
0
Nov 2010
Mar 2011
Jul 2011
Nov 2011
Mar 2012
Jul 2012
Nov 2012
Mar 2013
Jul 2013
Nov 2013

Exchanges


MtGox Exchange Rate
US Dollar / BTC
0
200
400
600
800
1000
1200
1400
Aug 2010
Dec 2010
Apr 2011
Aug 2011
Dec 2011
Apr 2012
Aug 2012
Dec 2012
Apr 2013
Aug 2013
Dec 2013

MT.GOX

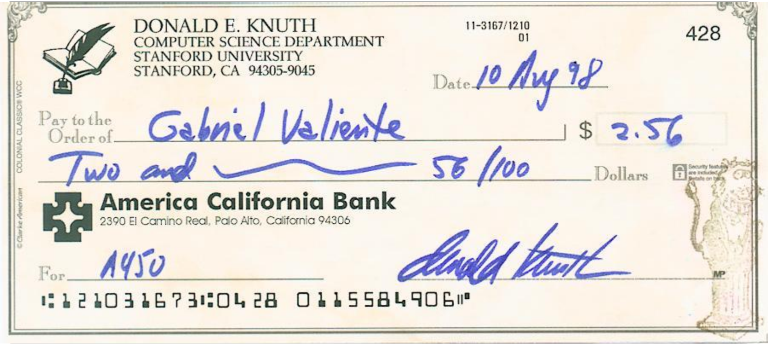
Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks.

The MtGox Incident

- July 2010: First trade on MtGox
- 2011: Transaction malleability identified as low priority issue
- February 7, 2014: MtGox halts withdrawals
- February 10, 2014: MtGox cites transaction malleability as root cause
- February 28, 2014: MtGox files for bankruptcy

MtGox claims that 850,000 bitcoins (620 million USD) were lost due to transaction malleability.

Transactions



DONALD E. KNUTH
COMPUTER SCIENCE DEPARTMENT
STANFORD UNIVERSITY
STANFORD, CA 94305-9045

11-3167/1210
01

428

Date 10 Aug 98

Pay to the Order of Gabriel Valiente $ 2.56

Two and 56/100 Dollars

Security features are included. Details on back.

America California Bank
2390 El Camino Real, Palo Alto, California 94306

For A450

Donald Knuth

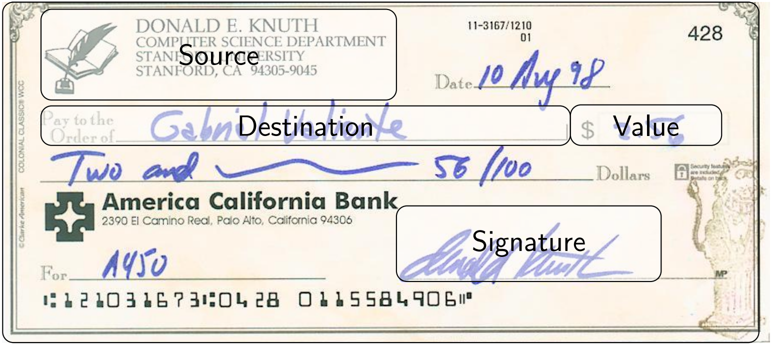
MP

⑆121031673⑆0428 0115584906⑈

COLONIAL CLASSIC® WCC

© Clarke American

Transactions



DONALD E. KNUTH
COMPUTER SCIENCE DEPARTMENT
STANFORD UNIVERSITY
STANFORD, CA 94305-9045

11-3167/1210
01

428

Date 10 Aug 98

Pay to the Order of Gabriel Valiente

$ 2.56

Two and ——— 56/100 Dollars

America California Bank
2390 El Camino Real, Palo Alto, California 94306

For A450

Donald Knuth

⑆121031673⑆0428 0115584906⑈

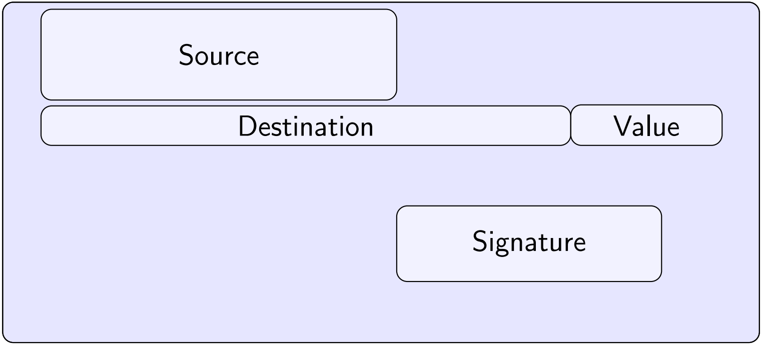
Source

Destination

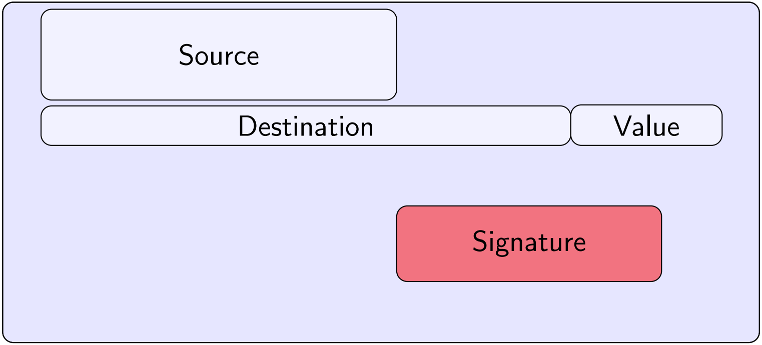
Value

Signature

Transactions



Transactions



Signatures

61 af bb 4d e9 f8 b8 74 86 1e

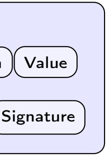
Signatures

00 00 61 af bb 4d e9 f8 b8 74 86 1e

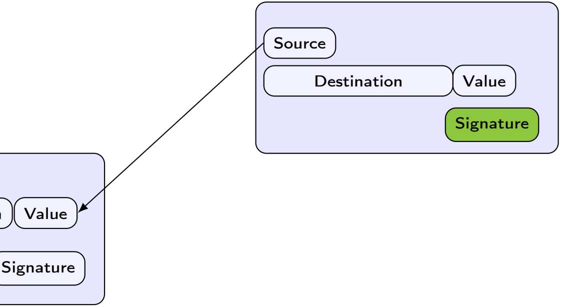
There are multiple ways to serialize a signature:

- Multiple push operations (1 byte, 2 byte, 4 byte)
- Non-canonical DER encodings
- Padding
- . . .

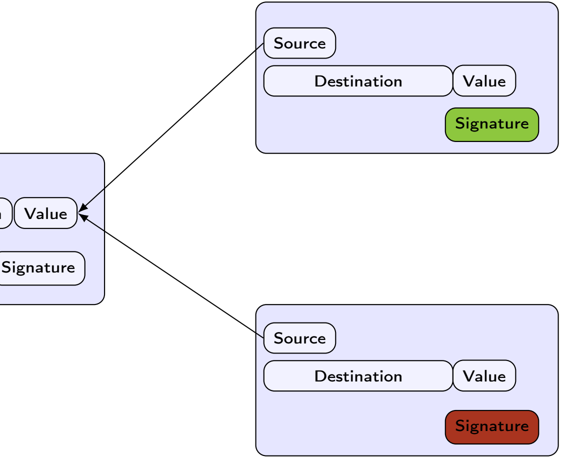
Doublespending



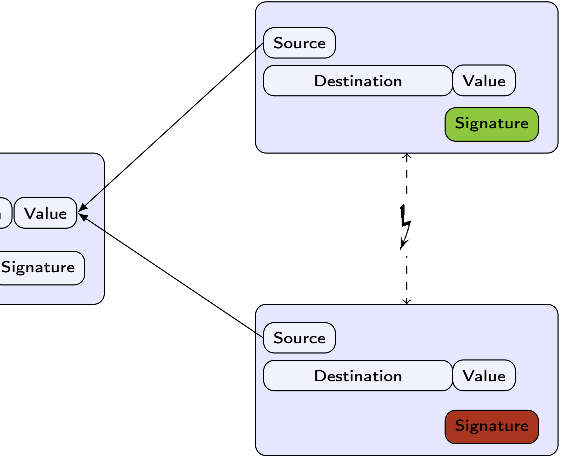
Doublespending



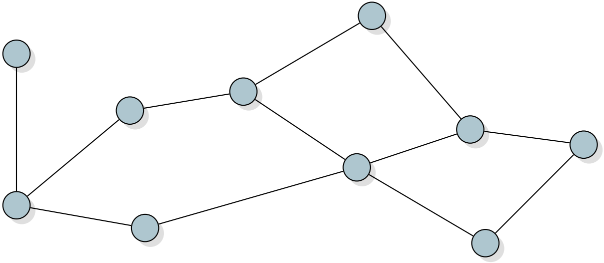
Doublespending



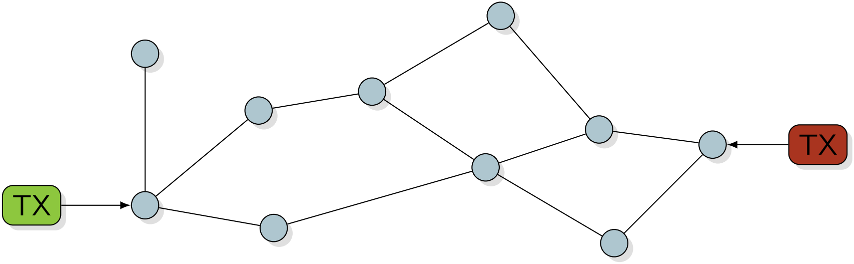
Doublespending



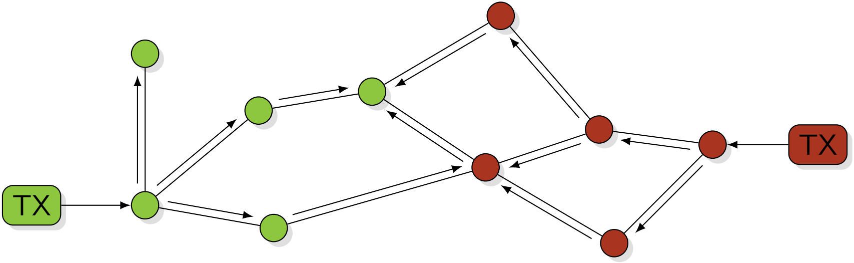
Transaction Conflicts



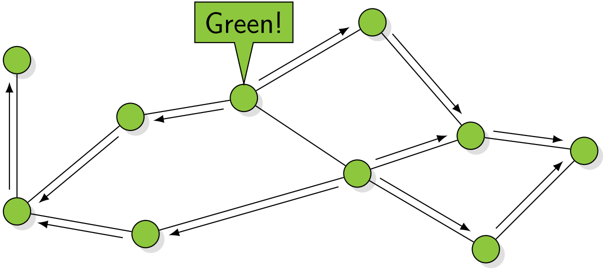
Transaction Conflicts



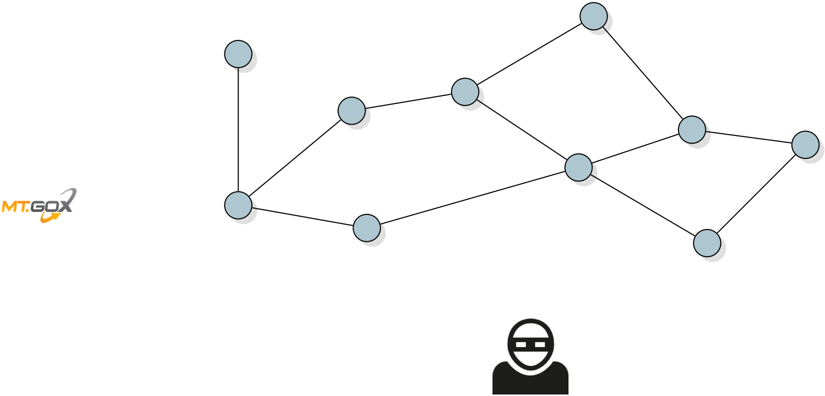
Transaction Conflicts



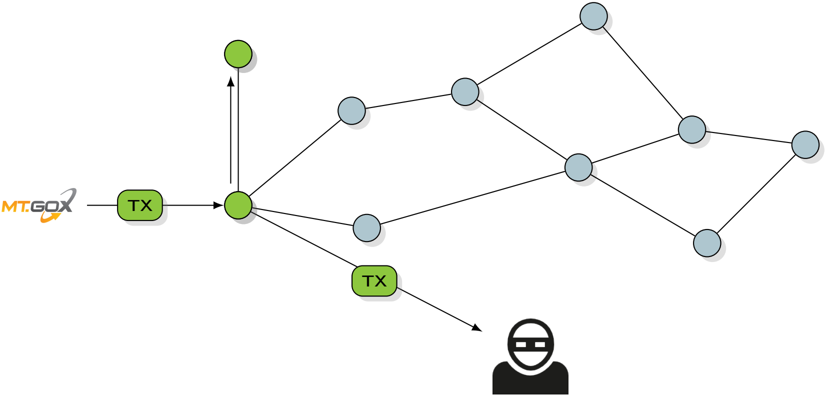
Transaction Conflicts



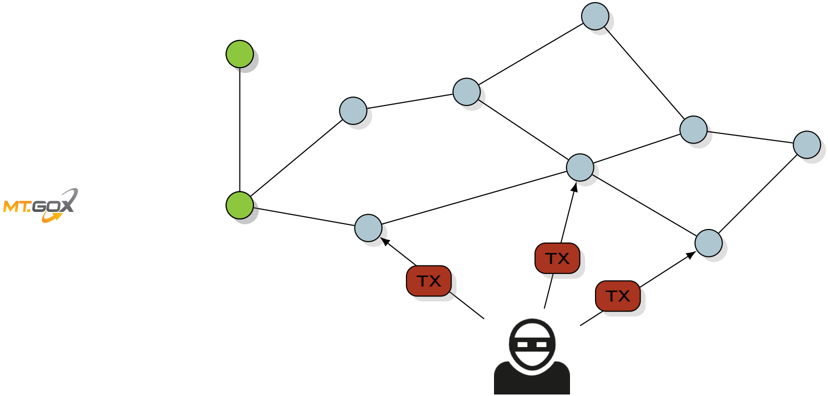
Transaction Malleability Attack



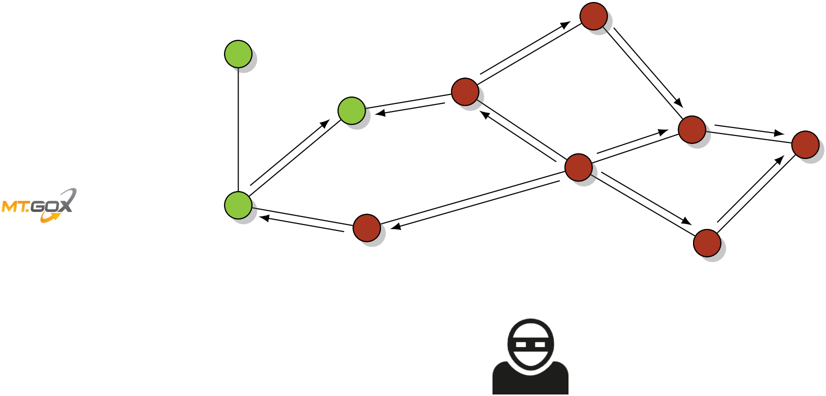
Transaction Malleability Attack



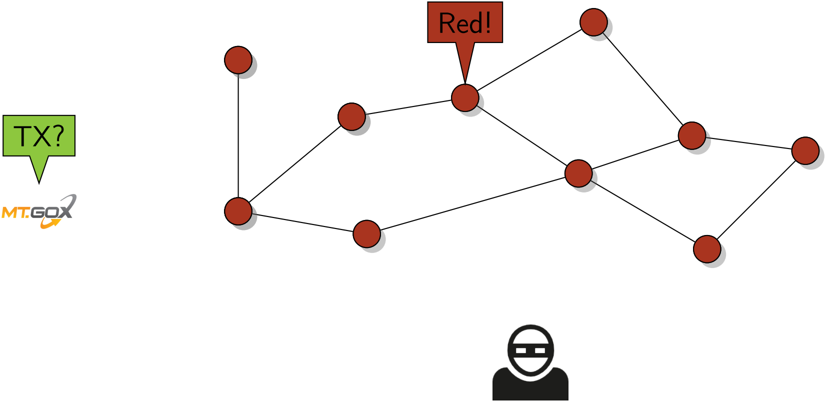
Transaction Malleability Attack



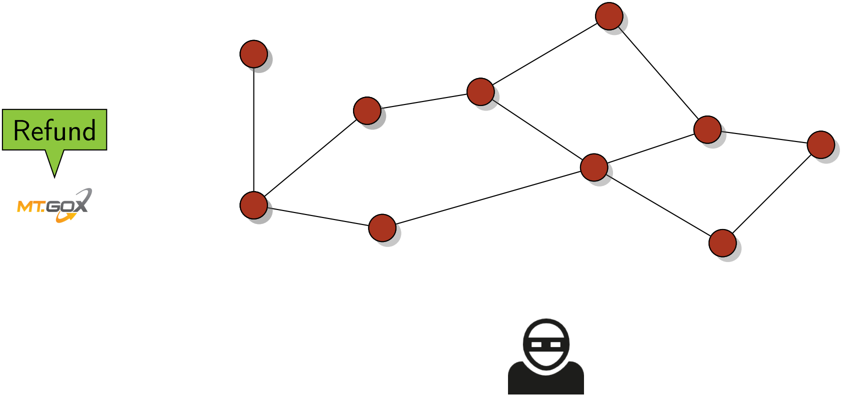
Transaction Malleability Attack



Transaction Malleability Attack



Transaction Malleability Attack



Data Gathering

Bitcoin can be monitored:

- Transactions are broadcast in the network;
- Conflicts can only be detected while they happen;
- Propagation is stopped when a conflict is detected;

Data Gathering

Bitcoin can be monitored:

- Transactions are broadcast in the network;
- Conflicts can only be detected while they happen;
- Propagation is stopped when a conflict is detected;

Connecting to a large sample allows collecting conflicts:

- Starting Jan. 2013 we collected transactions from the network;
- 1000 connections to random peers open;
- Network size 3,000 – 6,000 nodes;

Global Analysis

Conflict Set: set transactions that differ only in the signature.

- Total conflict sets: 35,202
- Conflict sets with one tx confirmed: 29,139
- Total involved bitcoins: 302,700 BTC

Global Analysis

Conflict Set: set transactions that differ only in the signature.

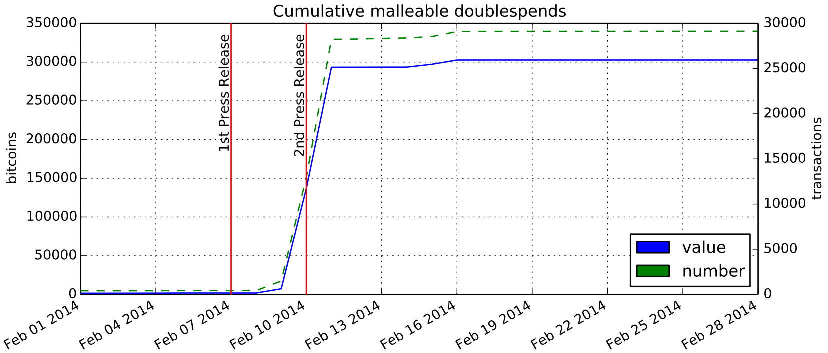
- Total conflict sets: 35,202
- Conflict sets with one tx confirmed: 29,139
- Total involved bitcoins: 302,700 BTC
- 28,595 sets involve OP_PUSHDATA2 opcode

Global Analysis

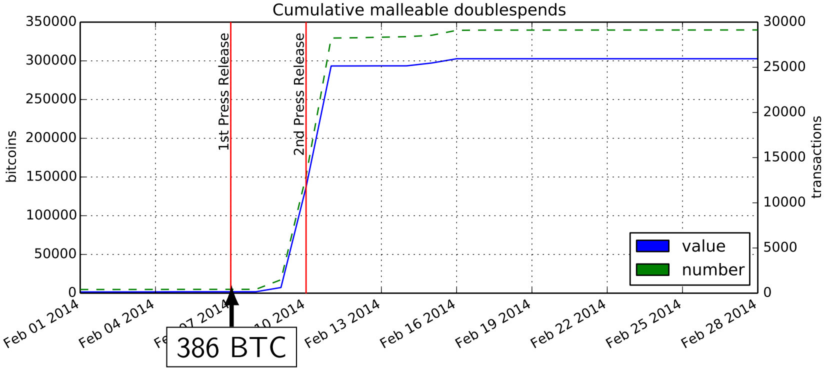
Conflict Set: set transactions that differ only in the signature.

- Total conflict sets: 35,202
- Conflict sets with one tx confirmed: 29,139
- Total involved bitcoins: 302,700 BTC
- 28,595 sets involve OP_PUSHDATA2 opcode
- Of the above instances 21.36% resulted in the modified transaction being confirmed

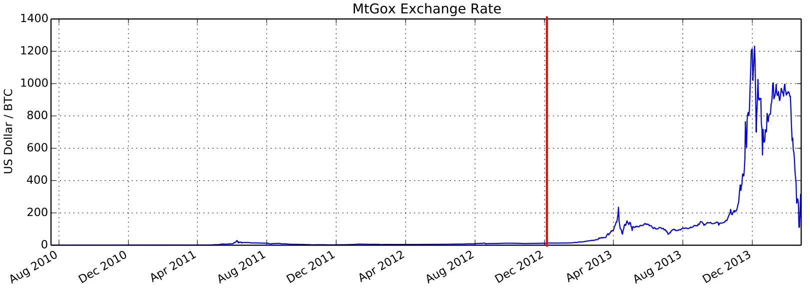
Incident Timeline



Incident Timeline

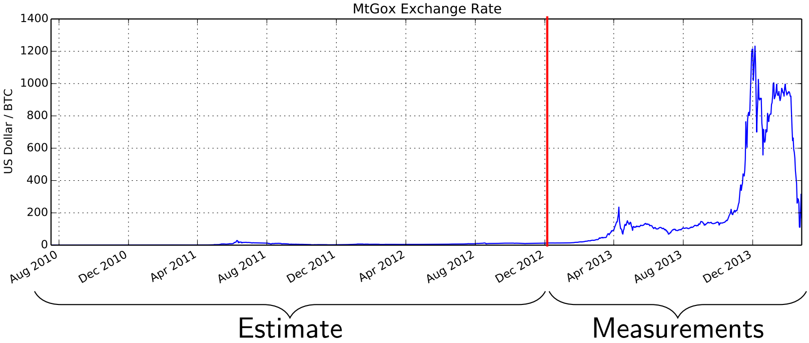


Beyond our Data



Measurements

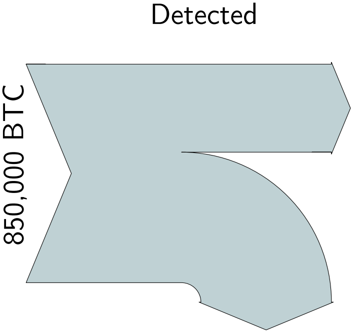
Beyond our Data



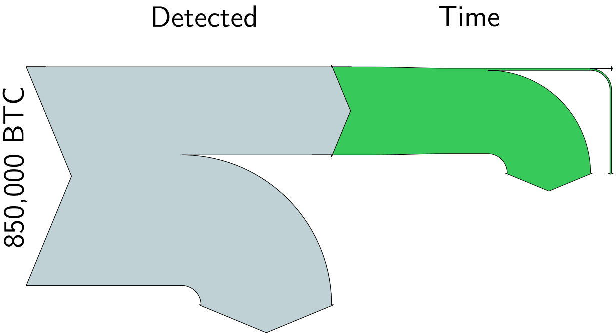
Estimate

Measurements

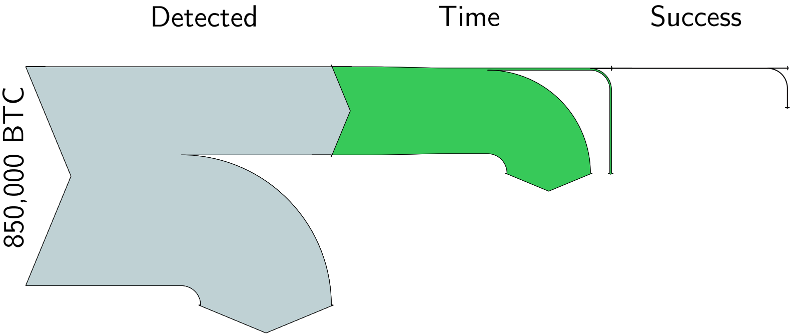
Conclusion



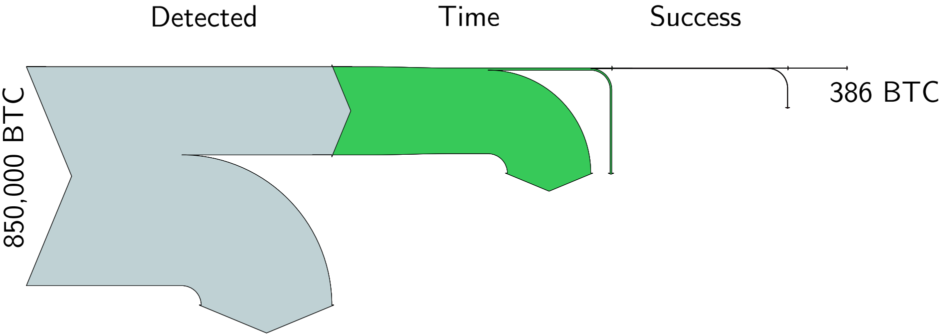
Conclusion



Conclusion



Conclusion



Thank you, questions?

Authors:
Christian Decker
Roger Wattenhofer