IC3 The Initiative For CryptoCurrencies & Contracts

UCL

Smart Contracts for Bribing Miners

Patrick McCorry, **Alexander Hicks**, Sarah Meiklejohn
University College London

What is a bribery attack?

A wealthy adversary seeks to rent hashrate from existing miners in order to obtain a majority of the network's computational power.

There are two methods to fund a bribe:

- In-band (e.g. large fees)
- Out-of-band (bank transfer; payment in another cryptocurrency)

If a sufficient portion of miners accept the bribe, then **the briber can censor, reverse or attack the cryptocurrency in question.**

Why would a miner accept a bribe?

Tragedy of the commons (Bonneau ‘16)

- All miners have an interest in the cryptocurrency’s long-term health
- Miners may deviate in the short-term to maximise their profit

Have we seen real-world examples of miners boosting short-term profit?

Potential bribery already?

Miners are getting subsidies

Another theory is that there may be bitcoin cash supporters that are subsidizing mining in some way, behind the scenes.

This could be something like an over-the-counter market for bitcoin cash where buyers are paying a higher price than the exchanges to incentivize mining. If the buyers demand freshly minted bitcoin cash, this would effectively make it so miners were the only supply that could satisfy this particular demand.

Similarly, bitcoin cash supporters could simply be paying pools to point hash power the blockchain network.

https://www.coindesk.com/miners-mining-bitcoin-cash-losing-money/

Any wealthy adversaries out there?

“We have prepared $100 million USD to kill the small fork of CoreCoin, no matter what proof of work algorithm, sha256 or scrypt or X11 or any other GPU algorithm. Show me your money. We very much welcome a CoreCoin change to POS.”

Zhuoer (BTC.TOP founder) in February 2017
He held **13% of the network’s computational power** as of October 2017

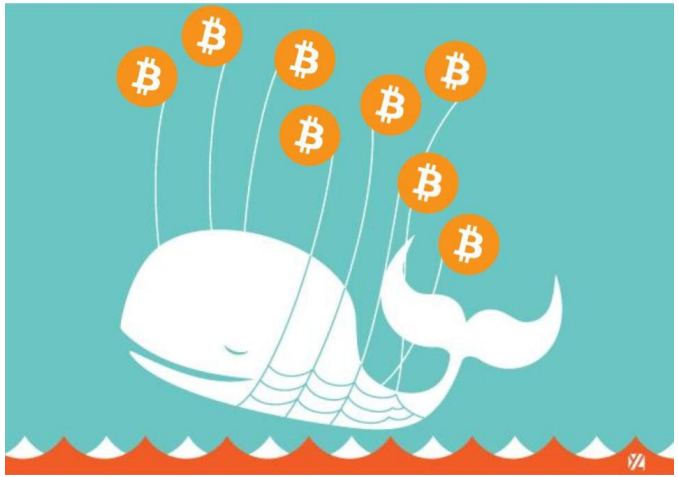
https://www.ccn.com/bitcoin-market-needs-big-blocks-says-founder-btc-top-mining-pool/

State of the art in “bribery-style attacks”

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘

Whale Transactions *(K. Liao and J. Katz)*

Briber signs transaction with anomalously large fee

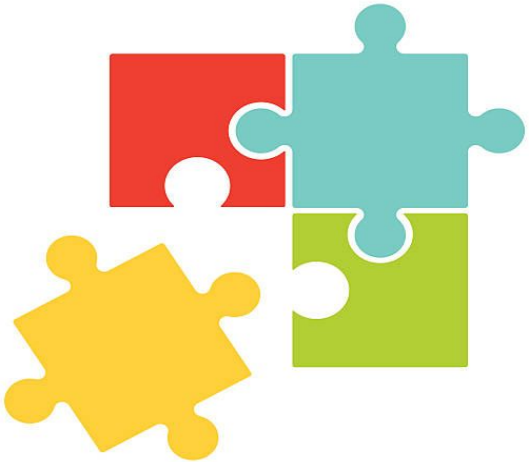


State of the art in “bribery-style attacks”

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘

Script Puzzles *(J. Teutsch, S. Jain, and P. Saxena)*

Briber publishs a PoW puzzle inside a transaction that sends the solver a large reward if solved.



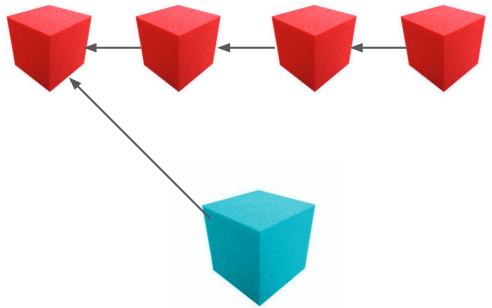
State of the art in “bribery-style attacks”

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘
Proof of stale block	✔ (Not fully)	✔	Out of band	✘

Proof of stale block *(L. Luu, Y. Velner, J. Teutsch, and P. Saxena)*

Smart contract rewards miners who can prove they mined a stale block in another cryptocurrency.

Trust Issue: cannot check if stale block is valid



Smart contracts remove the trust required between Briber and Miner

CensorshipCon

HistoryRevisionCon

GoldfingerCon

CensorshipCon

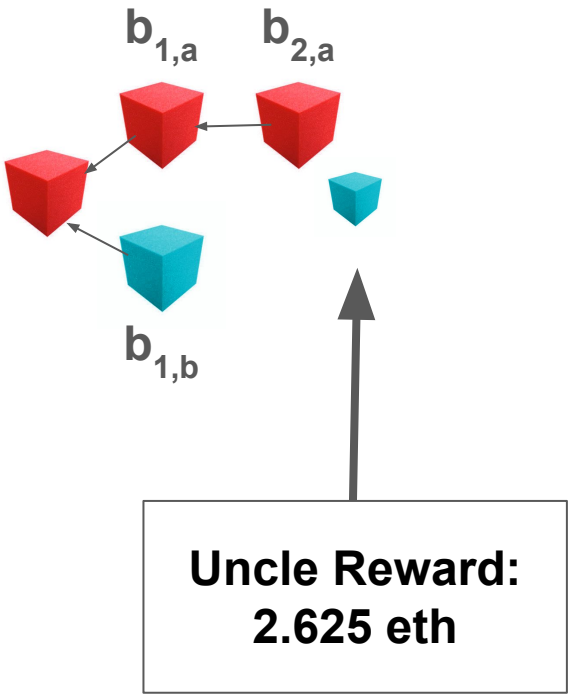
Briber wants full control over the blockchain and **they will be subsidised by the uncle block reward**

CensorshipCon

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘
Proof of stale block	✔ (Not fully)	✔	Out of band	✘
CensorshipCon	✔	✘	In band	✔

Trustless - Briber and Briber only trust the smart contract
Divert hashrate - All blocks contribution to the blockchain's overall weight
Subsidy - Uncle block reward policy subsidises the briber

What is an uncle block?

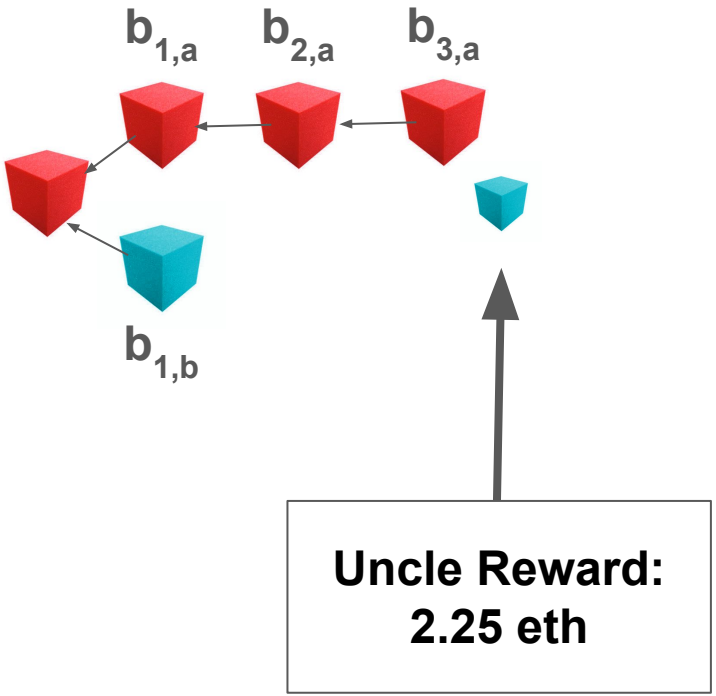


Ethereum added an “uncle block reward policy”

- All uncle blocks receive a **partial reward** depending on when it is accepted

Ethereum allows up to two uncle blocks per block

What is an uncle block?

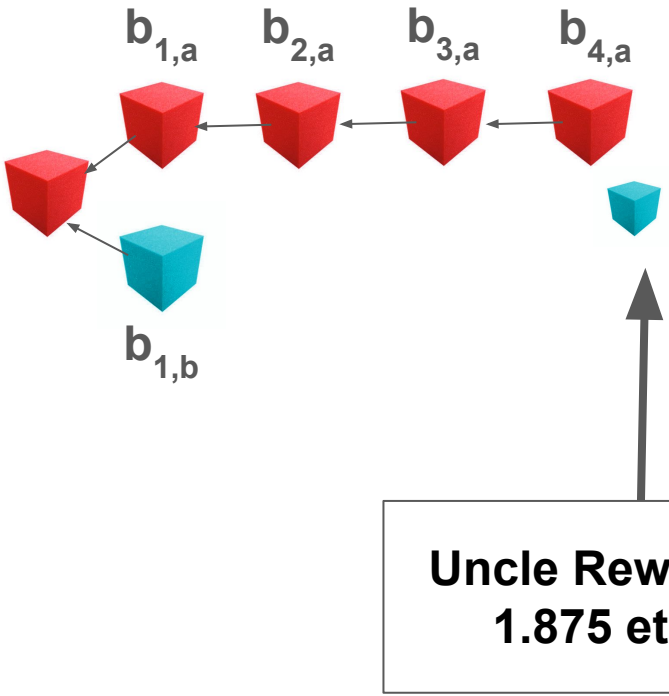


Ethereum added an “uncle block reward policy”

- All uncle blocks receive a **partial reward** depending on when it is accepted

Ethereum allows up to two uncle blocks per block

What is an uncle block?

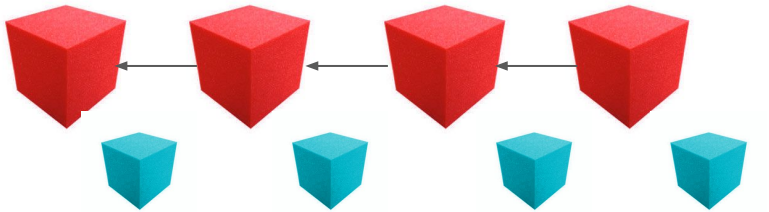


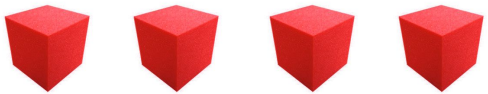
Ethereum added an “uncle block reward policy”

- All uncle blocks receive a **partial reward** depending on when it is accepted

Ethereum allows up to two uncle blocks per block

What will the blockchain look like during the attack?





Briber only creates main blocks

Bribed miners only create uncle blocks

CensorshipCon: Subsidy and Hashrate Requirement

For each uncle block:

- Network pays up to 2.625 ether.
- Briber pays remaining share of the block reward + the bribe bonus

Minimum initial hashrate:

- With >25%, not all miners can accept the bribe
- With >33%, all miners can accept the bribe

Briber and miners

HistoryRevisionCon

Briber wants to reverse / remove a transaction from the blockchain
by rewarding miners for **mining an alternative (and longer) fork**

HistoryRevisionCon

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘
Proof of stale block	✔ (Not fully)	✔	Out of band	✘
CensorshipCon	✔	✘	In band	✔
HistoryRevisionCon	✔	✘	In band	✔

Trustless - Briber and Briber only trust the smart contract
Divert hashrate - Only if the attack is not successful
Subsidy - Same trick as before - uncle blocks can subsidise attack

HistoryRevisionCon: Observations

Two modes of payment:

- Every block (full block reward + bribe)
- Every uncle block (subsidised block reward + bribe)

All or nothing:

- Bribed miners are only rewarded if new fork becomes the longest chain

Could be used for more than double spending:

- Inspecting the state of other contract, reversing computations and state transactions

Source: ETHnews

Could have saved the Parity wallets…

Source: ETHnews

…. Although bribery hard-fork smart contracts can still save the day …

i.e. reward miners 20% of the locked 519k ether for the next *k* blocks?

GoldfingerCon

Can Ethereum be used to **reduce the utility of Bitcoin?**

Goldfinger attacks

A wealthy adversary wants to reduce the utility of another cryptocurrency (Kroll, Davey, Felten at WEIS 2013)

Before: miners are invested in the utility of the cryptocurrency they mine, trust required between briber and miner

Now: many competing cryptocurrencies and smart contracts

GoldfingerCon

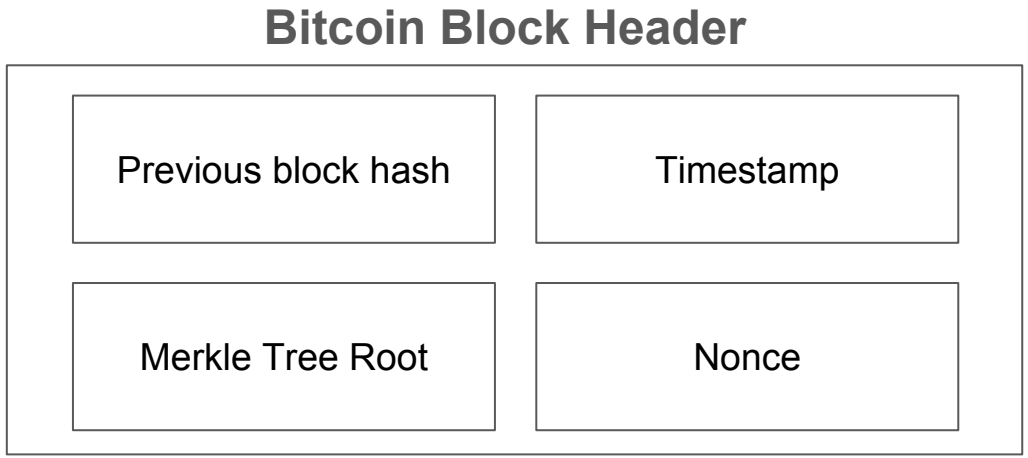
	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘
Proof of stale block	✘	✔	Out of band	✘
CensorshipCon	✔	✘	In band	✔
HistoryRevisionCon	✔	✘	In band	✔
GoldfingerCon	✔	✘	Out of band	✘

Trustless - Briber and Briber only trust the smart contract
Divert hashrate - All blocks are accepted into the attacked cryptocurrency
Subsidy - No uncle blocks

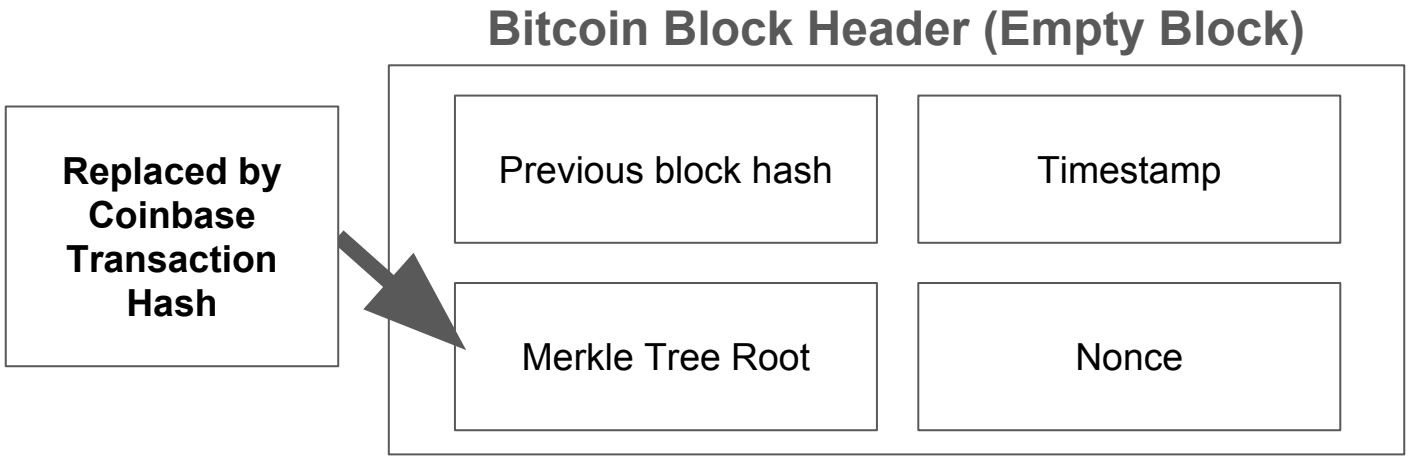
How can we reduce the utility of Bitcoin?

Easy - reward miners for mining empty blocks

… how to verify an empty block?



All empty blocks have the coinbase transaction hash in their headers….



GoldfingerCon: Proof of Concept Implementation

Purpose	Gas Cost	US$ Cost
Create Contract	3,505,654	4.21
Submit block header 49,996 (checkpoint)	316,799	0.38
Submit block header 50,000 (out of order)	276,799	0.33
Submit block header 49,999 (out of order)	261,727	0.31
Submit block header 49,998 (out of order)	261,727	0.31
Submit block header 49,997 (in order)	314,017	0.38
Accept bribe for block 50,000	152,529	0.18

Around **$0.56** to submit block header, coinbase transaction & accept bribe (October 2017)

State of the art in “bribery-style attacks”

	Trustless	Divert hashrate	Payment	Subsidy
Whale transactions	✘	✘	In band	✘
Script Puzzles	✔	✔	Both	✘
Proof of stale block	✘	✔	Out of band	✘
CensorshipCon	✔	✘	In band	✔
HistoryRevisionCon	✔	✘	In band	✔
GoldfingerCon	✔	✘	Out of band	✘

Future work

- What are the best strategies for ramping up the attack in order to achieve a majority of the hashrate?
  - Right now - we assume briber has managed to bribe a sufficient portion of miners
- What is the impact of selfish mining strategies in combination with bribery attacks for attacking and defending the network?
  - Rational miners vs bribed miners. Who will win?
- Can these bribery contracts be used in a proof-of-stake setting and is there any fundamental differences in the style of bribery?
  - Same coin can be used to both buy voting rights and pay bribes. Dangerous combo?

Summary

- CensorshipCon
  - Briber relies on the uncle block reward policy to subsidse the attack
- HistoryRevisionCon
  - Contract verifies that history was reversed before rewarding the miner
- GoldfingerCon
  - Rewards a miner in one cryptocurrency for reducing the utility in another cryptocurrency

Questions?

github.com/stonecoldpat/briberycontracts

alexander.hicks@ucl.ac.uk alexanderlhicks
p.mccorry@ucl.ac.uk paddyucl
s.meiklejohn@ucl.ac.uk