Bitcoin Redux

Ross Anderson, Ilia Shumailov, Mansoor Ahmed, Alessandro Rietmann

Cambridge

WEIS, Innsbruck, June 2018

BIS Annual report, June 17th

"Cryptocurrencies promise to replace trusted institutions with distributed ledger technology. Yet, looking beyond the hype, it is hard to identify a specific economic problem which they currently solve. Transactions are slow and costly, prone to congestion, and cannot scale with demand. The decentralised consensus behind the technology is also fragile and consumes vast amounts of energy. Still, distributed ledger technology could have promise in other applications. Policy responses need to prevent abuses while allowing further experimentation."

Regulation so far

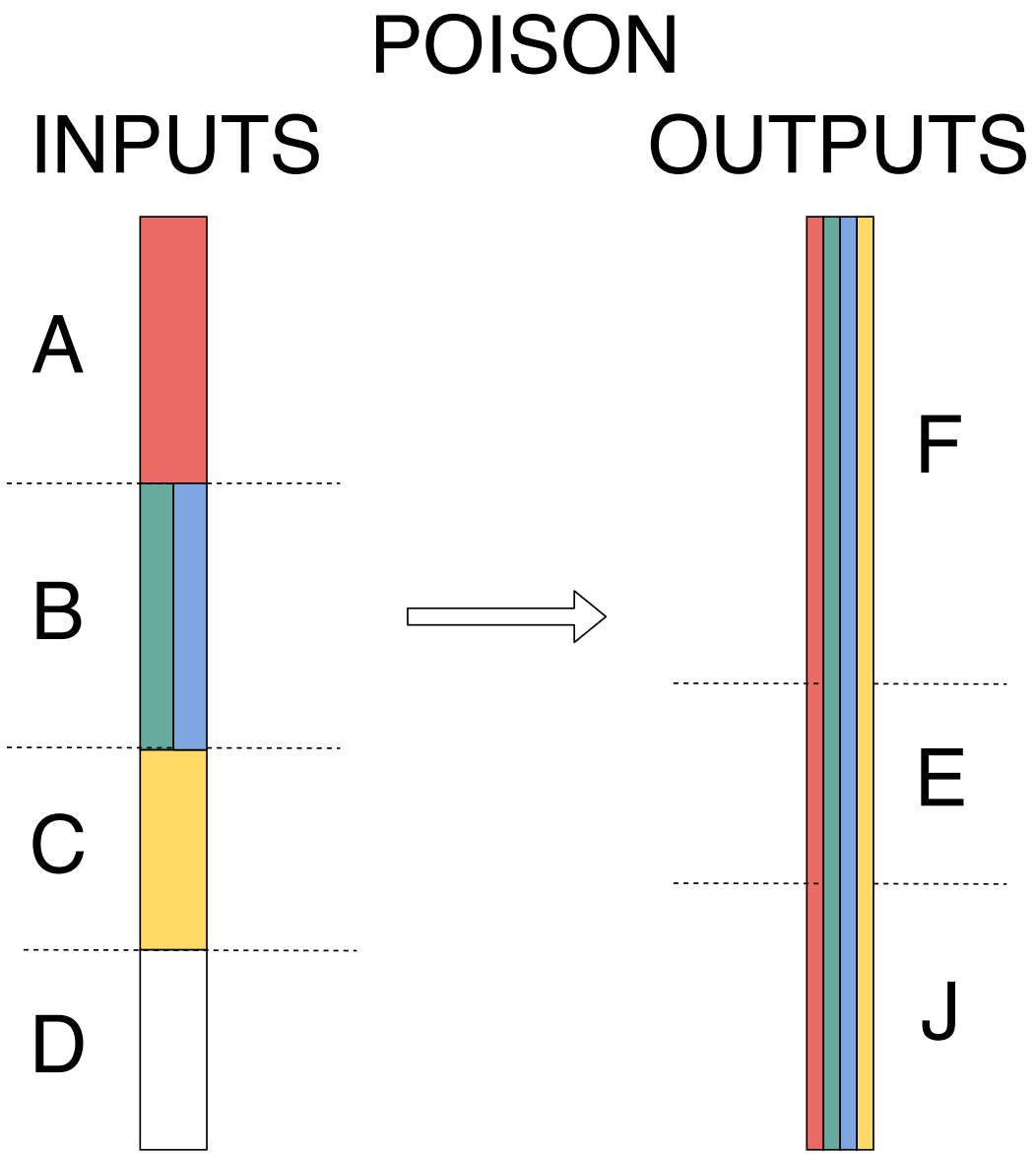
- Since 2013, FinCEN insists that exchanges register as money service businesses
- Since 2017, defaulters get raided
- Need know-your-customer not just to change BTC for $, but to change BTC for Eth
- 2018: EU Directive PE CONS 72/12 ‘tries’ to regulate wallet hosting service providers too
- Some governments have gone much further...

How can we track stolen coins?

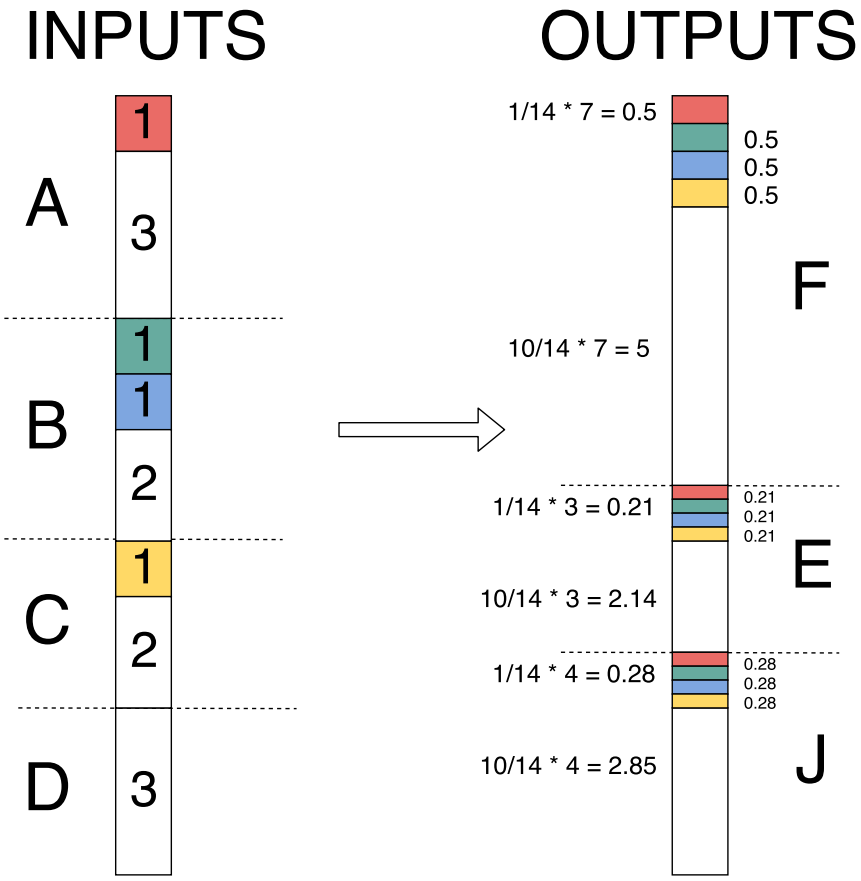
- Over 6% of bitcoin have been reported stolen
- Even more may be proceeds of other crimes
- The blockchain is public, so why not just track them and recover them from exchanges?
- Möser, Böhme, Breuker: poison or haircut?
- If you get Btc 3 stolen, then Btc 7 legal:
  - ‘Poison’ tainting gives you Btc 10 stolen
  - ‘Haircut’ gives you Btc 10, marked as 30% stolen

What English law actually says

- David Fox: when tracking funds to which there are mixed claims through an account, you have to use first-in-first-out (FIFO)
- "Clayton's case" – Devaynes v Noble, 35 ER 767, 781 (1816)
- This has spread from England to Commonwealth jurisdictions like Canada
- So we decided to measure the effect…

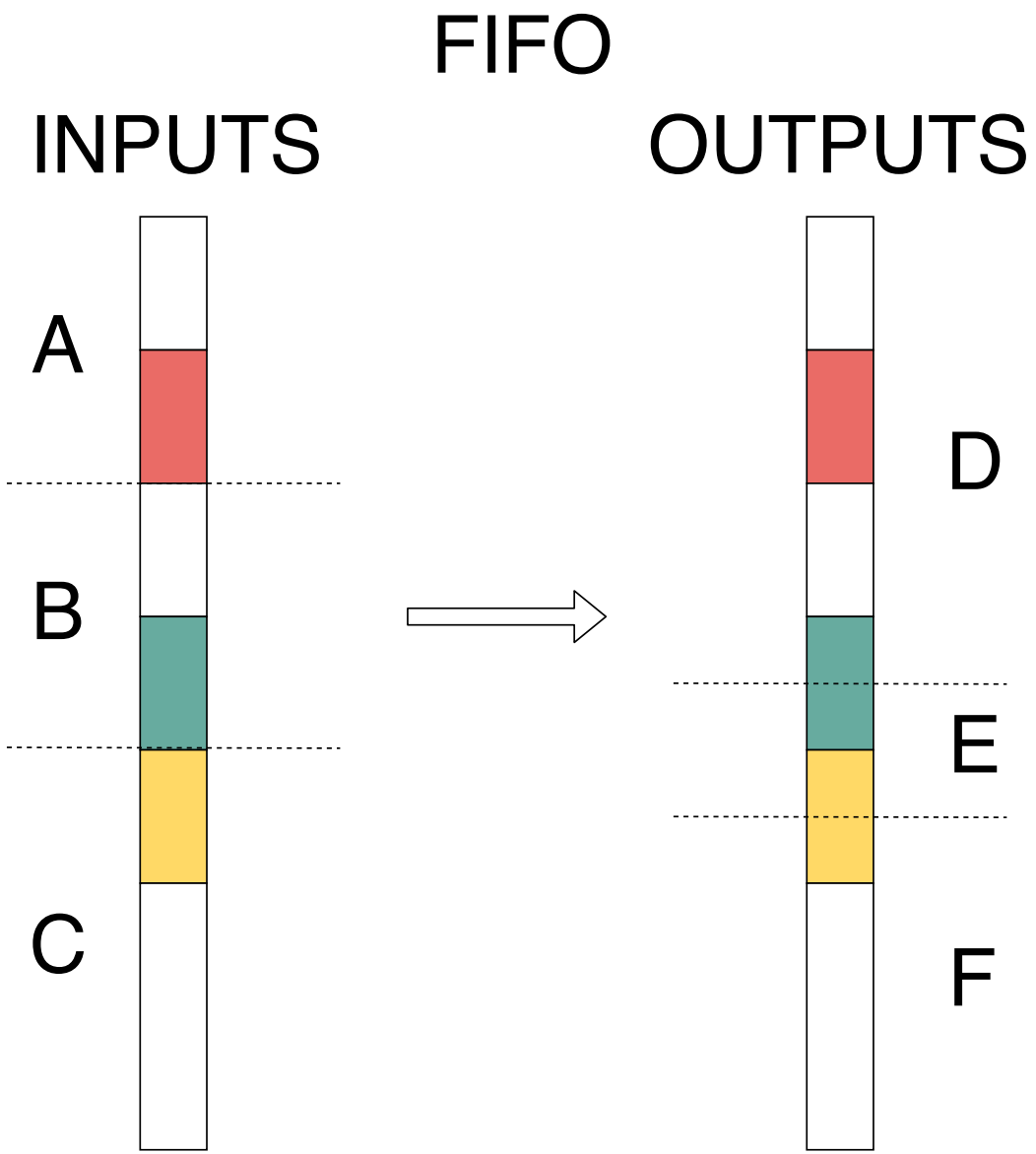

POISON
INPUTS
OUTPUTS
A
B
C
D
F
E
J

HAIRCUT



Overall: 14

Taint amount = outpoint value * taint % of the whole input


FIFO
INPUTS
OUTPUTS
A
B
C
D
E
F

Methodology + sample results

- We ran haircut and FIFO on bitcoin from the genesis to 2018 starting with 56 theft reports
- Linode: Btc 46,653 stolen in 2012, haircut now taints 16,855,619 addresses (93% of total)
- FIFO only taints 254,120 (1.3%)
- Flexcoin: Btc 896 stolen in 2014, haircut taints 10,421,122 addresses (57%)
- FIFO taints only 15,265

Why FIFO is better (2)

- Haircut tainting is lossy; can't go backwards
- FIFO tracking is lossless so tracing is reversible
- You can go forward from a stolen coin to all UTXOs it taints, or back from a UTXO to see its entire ancestry
- The handling of transaction fees is very different, as it's fiddly (but important)
- With FIFO, most UTXOs (72%) have no taint from our set of 56 well-publicised large thefts

Nemo dat quod non habet

- ‘You can’t give what you don’t own’
- If Bob steals Alice’s horse and sells it to Charlie, then when she sees him riding it she can demand it back
- There is no statute of limitations for theft, so long as bitcoin are just a commodity
- Bitcoin folks rely on the difficulty of tracing
- Their policy goal is ‘fungibility’

Nemo dat quod non habet (2)

- England used to have a ‘market overt’ loophole, but closed that in 1995
- Two exceptions for money. You can own it
  - If you got it in good faith for value
  - If you got it from a regulated bank
- Might these apply if bitcoin becomes money?
- Bitcoin folks lobby for bitcoin to be money, or for the blockchain to constitute ownership

Laundries

- What about bitcoin mixes or laundries?
- Idea: put one bad coin in a bag with nine good ones and then shake and choose or chop and change
- FIFO tainting makes the first unattractive
- And if you chop and join the coins into puff pastry, that's clear evidence of bad faith
- So even if bitcoin becomes money, laundries don't work as advertised!

How do we implement tracking?

- If bitcoin becomes money or a regulated exchange otherwise gives good title, its customers will want its addresses public
- But then theft victims can sue the exchange more easily
- And sellers will want to check their coins
- How can we fix this?

How do we implement tracking?

- If bitcoin becomes money or a regulated exchange otherwise gives good title, its customers will want its addresses public
- But then theft victims can sue the exchange more easily
- And sellers will want to check their coins
- How can we fix this?
- Coming soon: a public Taintchain!

Taint tracking in practice

- We publicised our FIFO approach in March (Security Protocols Workshop paper, video)
- We hoped to get lots of theft reports that we could follow up
- What we found: almost none of the victims had ever really owned a bitcoin!
- Starting with Mt. Gox, exchanges have been ‘hosting’ customers’ wallets

How can you own an asset?

- Self-hosting: keep your gold coins under the bed, or keep your private key on your laptop
- Gold merchant: you buy a gold bar for £30,000 and the merchant keeps it in their vault but with your name on it. If they go bust, it's still yours
- Bank: you deposit it and the bank now owes you £30,000. If it goes bust, you stand in line

How bitcoin really works now

- The exchanges suggest they're gold merchants but the blockchain suggests they're banks
- Huge growth in 'off-chain' transactions over the past 2 years; payments fast and cheap
- Now most people in US, UK use Coinbase, most Chinese use Binance etc
- They are acting as e-money providers but without the licences required by EU law
- The E-Money Directive is not being enforced

How regulation is failing

- EU: new definition of hosted wallet (a service holding keys) is two years out of date
- Germany is similar; closed OneCoin as it was transferring funds by adjusting Euro balances, but ignores off-chain bitcoin transactions
- UK: Financial Conduct Authority won't see payment as significant: bitcoin a 'crypto asset'
- So it won't give the Payment Service Regulator authority over cryptocurrency payments

Recommendations

- First and most important: EU governments must regulate exchanges offering off-chain payments under the E-money Directive
- Next, they should regulate the relationship between the exchange and its customers under the 2nd Payment Services Directive
- Next, they should stop regulated exchanges doing transfers to/from unregulated exchanges (those not even compliant with FinCEN)

Recommendations (continued)

- Governments should demand that exchanges make clear whether customer assets are kept distinct or pooled, and who's the owner, i.e. whether they are 'gold merchants' or 'banks'
- They should ban exchanges from dealing in cryptocurrencies specifically designed to evade money laundering controls
- They should require exchanges to be adequately capitalised, and develop accounting standards to support this

Is there an upside to cryptocurrency?

- If there is, it's probably in smart contracts
- See for example JP Morgan project (liveblog of FC18 keynote, on lightbluetouchpaper.org)
- If a smart contract were built on a bill of exchange, ownership would be like money
- With central bank backing, even better!
- We recommend: if any central bank issues a cryptocurrency, it should support smart contracts and be redeemable at par

Finally – saving the planet

- Cryptocurrency mining now costs about 7GW, or as much as Israel
- It doesn't have to be this way!
- Plenty proposals for proof-of-X
- Enterprise ethereum uses Byzantine methods
- Our eighth recommendation: governments should impose a carbon tax at least equivalent to the €33 per tonne floor of the EU Emissions Trading Scheme

Conclusions

- We tried to undermine bitcoin fungibility by developing better taint-tracking tools
- We waited for bitcoin theft victims to come
- But almost none of them ever owned a bitcoin! (so the 5th AML directive misses the mark)
- The real problems are with the ecosystem
- Exchanges act as “banks”, pretend to be “gold merchants”, and ignore the law, with the tacit connivance of bank regulators
- Solution: enforce the laws we already have