The security economics of cryptocurrencies

Ross Anderson

Cambridge

Financial Crypto, Borneo, February 2020

Security economics

- If Alice guards a system and Bob pays the cost of failure, you can expect trouble!
- Example: managing card fraud takes effort by the merchant and the bank that acquires their transactions
- However, much of the cost of fraud falls on the customer and the bank that issued their card
- Large-system failures involve incentives, governance … and adversarial liability games
- Security economics has been a research topic for almost 20 years

Security economics and cryptocurrency

- We've been trying for 40 years to create a 'trusted computer' – from the Orange Book through HSMs and smartcards to enclaves
- The bitcoin blockchain finally gave us a global trusted computer!
- But it's built out of very strange components – a hardware monopoly, five mining gangs, a few dominant exchanges …
- What makes it work is the economics!
- At the transaction level, things are sort-of incentive compatible
- But there's more to it than the basic game theory!

Crypto and liability engineering

- All crypto that's used at scale becomes entangled with liability
- FDE – so if you leave your laptop on the train, you don't have to notify 8 million data subjects
- EMV – rolled out ten years earlier in Europe than in the USA because governments allowed banks to shift liability to merchants
- HSMs – the hardware may be secure but the internal apps often aren't. But banks still use them for compliance
- eIDAS mixed up ID cards with lawyers' income, tax returns, Docusign
- Can blockchains escape this?

How the crypto industry hacks the regulators

- Britain's Financial Conduct Authority says bitcoin is a 'crypto asset' as investment demand is much greater than transaction demand
- So it won't give the Payment Service Regulator authority over cryptocurrency payments (or use the EU term 'virtual currency')
- Germany is similar: it closed OneCoin as it was transferring funds by adjusting Euro balances, but ignores off-chain bitcoin transactions
- EU 5th AML directive tries to catch up, but its new definition of hosted wallet (a service holding keys) is seven years out of date
- Why should exchanges exempt from PSR not work like stockbrokers?

Our 2018 experiment

- We wrote better software to track stolen bitcoin (the Taintchain)
- Hope: victims of theft could trace their stolen coins and sue Coinbase to get them back
- Reality: almost no theft victims had ever actually owned a bitcoin!
- Starting with Mt Gox we've had the 'custodial exchange': the customer bitcoin are all in one pool
- Just as gold merchants in the 18th century became banks, you no longer keep your gold there, but have a claim on their gold

Two types of off-chain transaction

- Technical: Lightning (had many papers yesterday)
- Administrative: If I have an account at Coinbase and so do you, I transfer bitcoin to you by clicking on their web page
- The action's on their customer ledger, not on the blockchain ledger
- What are the relative transaction volumes??
- Most people in US, UK use Coinbase, most Chinese use Binance etc
- They're acting as e-money providers but without a licence
- The E-Money Directive is not being enforced

Other effects

- Allison talked on Monday about exchanges not caring about authenticating customers properly. Why is this?
- Why should exchanges promote Lightning? Is it about leaving custody (and thus liability) with the customer?
- Can you still support individual freedom and be against controls on cryptography, without having to put up with monopolistic abuses from market rigging to nonexistent customer care?
- Absolutely! Just because you support free software, doesn’t mean you have to support Google

Recommendations we made in 2018

- EU governments should apply the law – the E-money Directive – to exchanges offering off-chain payments
- Then the 2nd Payment Services Directive on the relationship between the exchange and its customers (i.e. 2FA)
- They should stop regulated exchanges doing transfers to/from exchanges that are not even compliant with FinCEN
- They should develop proper accounting standards (since then, much DeFi has been developing around tax planning)
- Governments should impose a carbon tax at least equivalent to the €33 per tonne floor of the EU Emissions Trading Scheme

Conclusions

- As cryptocurrencies have scaled up enough to matter, there are new stakeholders that the research community tends to ignore
- Lawyers are anti-security engineers. Their job is to enable their client to take risks at your expense
- Regulators in theory try to be the opposite, so that the risks end up with the stakeholders most able to bear them
- The next level game is that powerful stakeholders try to capture the regulators. This has already been happening
- The research horizon maybe needs to be a bit wider