Bitcoin in the Counter-Economy

Frank Braun

September 16, 2012

Who am I

- computer science background
- IT security consultant, will work for Bitcoin
- libertarian, pro free-markets
- interested in Austrian economics

$\Rightarrow$ *freedom technology*

What's up with the mask?

- privacy is necessary for liberty
- privacy is not granted, it has to be taken
- extreme surveillance requires extreme countermeasures

$\Rightarrow$ privacy extremist

Bitcoin in the Counter-Econonmy

this talk is **not** about privacy, but about

- What is the Counter-Economy?
- What has Bitcoin to do with it?
- Why is Bitcoin an important step towards a free society?
- What can **you do** to make Bitcoin succeed in the *long-run*?

$\Rightarrow$ 3 hypotheses

Counter-Economy in general (a.k.a. the black market)

- "Forget China: the $10 trillion global black market is the world's fastest growing economy – and its future. "
- "[If it] were an independent nation, united in a single political structure – call it the United Street Sellers Republic (USSR) or, perhaps, Bazaaristan – it would be an economic superpower, the second-largest economy in the world (the United States, with a GDP of $14 trillion, is numero uno)."
- "In the developing world, it's been increasing every year since the 1990s, and in many countries it's growing faster than the officially recognized gross domestic product (GDP)."

(The Shadow Superpower, *Foreign Policy*, October 28, 2011)

Crypto-Anarchy / Counter-Economics

- "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. [...] These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."
  (Timothy C. May, A Crypto Anarchist Manifesto)
- Crypto-Anarchy is **not** a philosophical utopia, but the attempt to shape life and society with **disruptive technologies**
- Fork in the road: total surveillance state or a crypto-anarchist libertopia?
- People with computers vs. the state

Bitcoin for a free society

- a free society needs a free market
- a free market needs sound money
- Bitcoin is money with good properties
  - pseudonymous
  - no frozen accounts
  - no charge-backs
  - very cheap and very fast transfer of funds

$\Rightarrow$ huge advantage over a barter or cash-only economy
(developed economies need money transfer, at least for B2B)

What does Bitcoin need to succeed in the long-run?

3 hypotheses (in short):

1. no state
2. no banks
3. OTC

3 hypotheses (in detail):

1. We should **not** try to get legality for Bitcoin, we should **not** ask the state to resolve conflicts in the community.
2. We should **not** focus on interoperability with the traditional banking system.
3. Widespread availability of over-the-counter (OTC) Bitcoin exchangers is crucial for Bitcoin to succeed in the long-run and give us more freedom.

Public choice theory

- people will do what is in their own self-interest
- this **includes** politicians, banksters, and cops
- (let me repeat that)
- don't assume your interests are their interest, they are **not**!

The state

A regional monopoly of force which extracts resources (i.e., money) from its sheeple to

1. mainly finance itself, its wars and its surveillance apparatus
2. uses the rest to provide "services" which could be provided better and cheaper by the free market

Money sources of the state:

1. taxation
2. monopoly of the money supply (via inflation your money becomes worth less)

The latter is better (sheeple don't notice)!

The state + public choice + Bitcoin = trouble

Bitcoin prevents inflation and helps tax evation (the system itself is hard to regulate)

$\Rightarrow$ potentially life-threatening to the state

$\Rightarrow$ the state will fight it **heavily** once he realises that

It is absolutely ludicrous to think that the state will embrace Bitcoin.

$\Rightarrow$ Hypothesis 1: We should **not** try to get legality for Bitcoin, we should **not** ask the state to resolve conflicts in the community.

History lesson: e-gold

- e-gold was a digital gold currency that allowed the instant transfer of gold ownership between 1996 and 2009
- they sought compliance with financial regulations
- a flourishing ecosystem existed around e-gold
- exchangers were attacked and closed down due to regulatory problems
- e-gold indicted on violating money laundering regulations and was ultimately closed down

$\Rightarrow$ Bitcoin *exchangers* will be attacked via state regulations

(although the Bitcoin network itself is harder to attack than e-gold)

Banks

- beneficiaries of fractional-reserve banking
- can borrow cheaply from central bank
- operate in the most heavily regulated industry
- $\Rightarrow$ huge barriers to entry (try to open a bank!)
- $\Rightarrow$ not much competition
- $\Rightarrow$ large profits ($$$)
- think transaction fees, credit cart fees, PayPal, Western Union, Money Gram, ...

Bitcoin **threatens this profits** and poses a **regulatory risk**

$\Rightarrow$ Bitcoin exchangers will be attacked by competing financial institutions (remember TradeHill?)

No banks

"A widely successfull Bitcoin system is against the self-interests of the established financial industry and it makes no sense for them to deal with the corresponding regulatory challenges in the long-run." (Frank Braun, 2012)

If the Bitcoin economy depends on the traditional banking system it is **doomed to fail**. (Think Mt. Gox!)

$\Rightarrow$ Hypothesis 2: We should **not** focus on interoperability with the traditional banking system.

The case for OTC

- the state is opposed to Bitcoin
- the traditional financial industry is opposed to Bitcoin
- $\Rightarrow$ we need a completely separate system of exchange
- $\Rightarrow$ a network of over-the-counter (OTC) exchangers
- OTC is: two people meeting **face-to-face** trading BTC for cash (or gold/silver)
- OTC is **not**: sending cash in the mail, wire-transfer, ...
- a widespread network of OTC exchangers is the system most resilient against state attacks (banking is skipped)
- if and only if the OTCs deal **securely** and **professionally**

$\Rightarrow$ Hypothesis 3: Widespread availability of OTC Bitcoin exchangers is crucial for Bitcoin to succeed in the long-run and give us more freedom.

Secure and professional OTC

- two enemies: the state and evil customers (e.g., fraudsters)
- $\Rightarrow$ risk mitigation (drive up the cost of a successfull attack)

two categories of techniques:

1. secure IT infrastructure (privacy FTW!)
2. tradecraft

Secure IT for OTCs

secure IT / privacy basics:

- use email encryption (PGP)
- use disk encryption
- use IP address anonymization (e.g., with TOR)
- use (multiple) **pseudonyms**

OTC deal basics:

- arrange OTC deal completely electronic
- e.g., use `bitcoin-otc.com` or `localbitcoins.com`
- agree on price and amount beforehand
- limit transaction size (only what you could afford to loose)
- the actual meeting only finalizes the deal, **no deviation!**

Digital arrangement protects against the state: less evidence and harder to prove

Tradecraft for OTCs

Tradecraft is skill acquired through experience in a (typically clandestine) trade.

For OTC:

- meet in public places **during the day** (e.g., a café)
- money is kept or on the table until the Bitcoin are transferred
- only the needed amount of Bitcoin on the client
- don't leave the protected public places with the money!

Methods:

- brush: give money to second person unnoticed (beware of the toilet)
- drop/cache: secure place to put the money (secure mailbox/door)
- deposit the money: go directly to the bank, but think of cash card (send it by mail, 3 wrong PIN attempts)
- safe deposit box (access)

Next level OTC

- use two persons for a deal, give money to backup
- separate buying BTC from selling BTC: until BTC is not a currency it is selling/buying and not money changing
- if Bitcoin becomes a currency, use goods of exchange (gold or silver)

Be professional:

- a professional dealer has professional prices (professionalism has its cost)
- don't cut corners to safe costs, this will defeat you long-term
- explain the benefits of a professional dealer to your customers
- if your fee is significantly $< 5\%$, you are either dealing very large amounts or you are fooling yourself

Conclusion

For Bitcoin to succeed long-term we need a large OTC ecosystem.

- Appeal: Stop lobbying, start acting.

$\Rightarrow$ Become an OTC exchanger today!

Acknowledgments: Jonathan Logan

Contacts:

- For all things privacy: `http://shadowlife.cc` (Oct 2012)
- Mail: `frank@cryptogroup.net` (please use PGP)
- Key: `0xCEC00E94`

Thank you for your attention! Questions?