
Mitigate the Devastating Effects of Crime Economy Through Eradicating Bitcoin

Jens Getreu, Tallinn University of Technology

Revision History

Revision 1.0

05/11/16

Abstract

This note first analysis the preconditions for a successful regulation policy on new information technologies. We explain how the new crime economy, based on anonymous division of labour, works. By going back in history we understand that controlling the money flow is the key to mitigate organized crime. Applied to our generation the author argues, that the most efficient way to fight against this new age of crime economy is to eradicate Bitcoin by prohibiting mining.

How to establish a successful regulation policy on new information technologies?

New technology can change society for better or for worse. Empowered by advances in information technologies new unethical activities emerged, partly because of the ease to operate anonymously from distance, but also because of the low risk of getting caught. There is a clear recognition that information technology regulation should combat international crime and, that it needs the full participation and commitment of all parties, including the government sector. But why are regulation policies often set up too late, after substantial damage has occurred already?

The reason is, that the cause effect relationship between technical innovation and social consequences is very complex. It involves the human being as consumer of technology and its individual rationality. His individual objectives lead to technology selection, which will affect the society as such. The [Figure 1, "A general model of ethics with technology selection"](#) [7] presents a schematic diagram of an extended ethics decision making model that includes the factor of technology selection. It combines the psycholog-

Mitigate the Devastating Effects of Crime Economy Through Eradicating Bitcoin

ical aspects of the individual reality with the sociological consequences of technology selection.

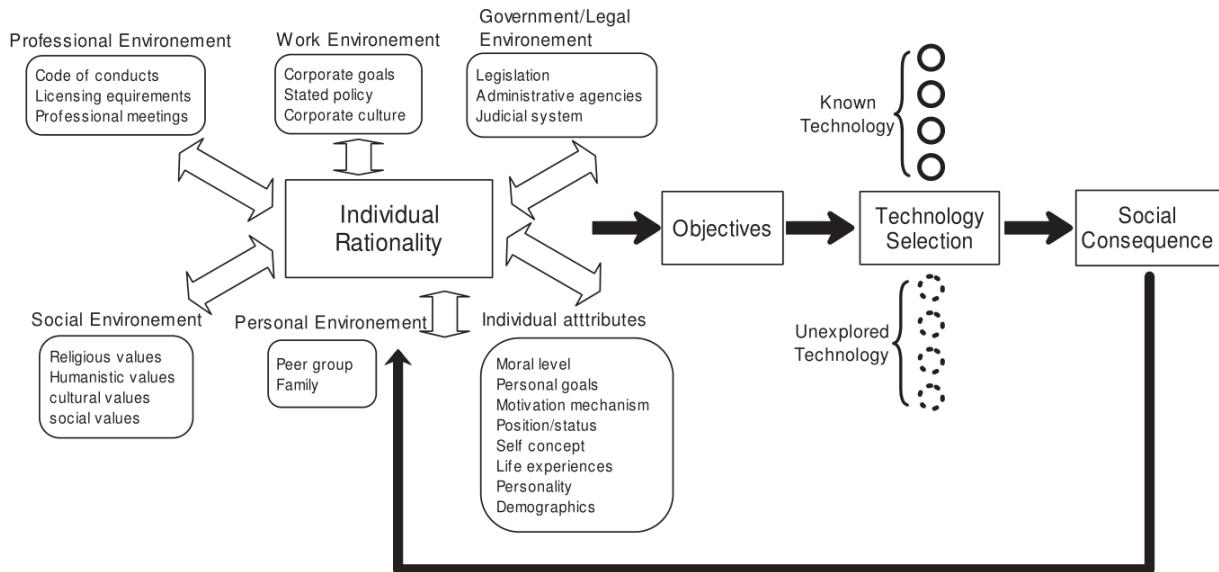


Figure 1. A general model of ethics with technology selection

It has to be noted that the above model does not rely on any definition of ethical or unethical behaviour. Knowing that any efficient regulation policy depend on the understanding of all components of the above control loop, a model of the individual rationality is essential. The model does not need to be universal, it can be limited and describe only one certain group of unethical individuals. Applied to unethical business manager Zhou [7] states:

Without loss of generality, we assume that in a common-sense business world, practitioners don't get involved in unethical activities unless they receive positive turnover by extracting the cost of unethical conduct from possible gains. The cost includes both the operational cost that is used to accomplish the activities and the opportunity cost that represents possible penalty if their unethical conduct is exposed. Practitioners then need to consider the options of technologies/means that they may use to achieve unethical goals, given certain operational cost for each choice.

Zhou [7] describes business manager as perfect economic entities: their individual rationality is targeted on maximising profit. This model must be adjusted to the target group. Concerning religious extremists, especially during war times, for example other assumptions have to be made.

Knowing your adversary is not the difficulty in modelling the cause effect relationships in the [Figure 1, “A general model of ethics with technology selection”](#): also the impact of unexplored technologies on society (“Technology Selection” → “Social Consequence”) is as difficult to predict!

Let’s assume that all details in the [Figure 1, “A general model of ethics with technology selection”](#) are sufficiently understood by the scientific society the next question arises: Where to interfere efficiently in the control loop? In theory all boxes in the above figure are valid leverage candidates, but practical and financial considerations will often restrict the actions to influence the “legal environment” or the “technology selection”. Thus, a possible solution could be, e.g. to maximize the deterrence of unethical activities via technology regulation.

Once the right leverage is found and translated into a regulative policy, political persuasion is required. Again, this is not as easy as one may assume: The highly technological implications can be misunderstood easily by decision makers and by voters.

The next chapter illustrates the methodology by analysing the relation “Bitcoin” (Technology Selection) with “Crime” (Social Consequence).

“Crime Economy” as social consequence of the technology selection “Bitcoin”

This section discusses the change in organized crime since the emergence of anonymous crypto-currencies like Bitcoin, which allow essential functions in criminal operations being outsourced. Starting from the technical principals of Bitcoin the impact on self-organisation of criminal entities are shown.

Defending against cyber crime becomes a more and more complex task: Organisations need to hire talented people, train and reward them. They have to establish a cybersecurity risk management system and set up technical environments and operations in order to maintain vigilance, respond to intrusions and to be prepared to restore critical services.

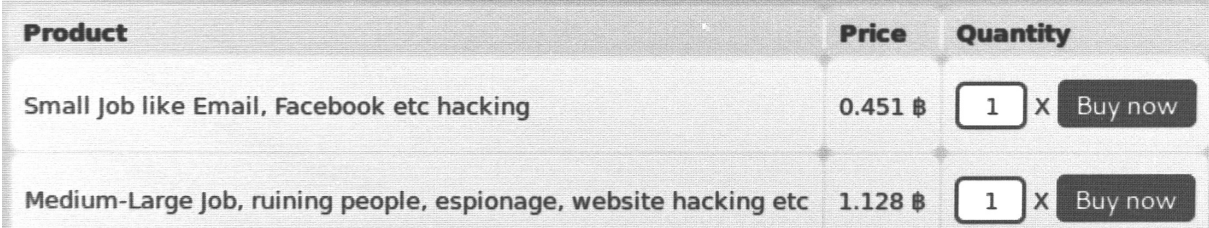
On the other hand planing, preparing and executing sophisticated cyber attacks is not less resource expensive. It also requires the cooperation of talented people as they have to offer services similar to those present in legal enterprises: finance, production, human resource management, communi-

Mitigate the Devastating Effects of Crime Economy Through Eradicating Bitcoin

cation and governance. The first criminal organisational structures providing these internal services appeared in the 20th century: For example: it is estimated that by 1929, Al Capone's income from the various aspects of his business was \$60,000,000 (illegal alcohol), \$25,000,000 (gambling establishments), \$10,000,000 (vice) and \$10,000,000 from various other rackets. It is claimed that Capone was employing over 600 gangsters to protect this business from rival gangs [5]

The early forms of organized crime were characterized by strongly authoritarian hierarchies and top down communication. With the emergence of new confidential electronic communication channels alternative forms of criminal organisations appeared. Bureaucratic and corporate criminal organisations for example developed extensive division of labour within the organisation. Even though, confidential electronic communication allowed the highly specialized units to cooperate the overall structure remained rigid. The reason is that the remuneration of internal services causes money flow within the organization. As long as the money transfer is mainly based on trusted non-anonymous personal relations, the organisation stays rigid. Establishing a network of trusted relations needs time and once it is in place is hard to change. It has to be noted that cash flow had always been the critical part in criminal transactions. This is partly due to simple logistical problems. For example, in 1997, the [U.S.] Justice Department estimated that every pound of cocaine sold on the street generated six pounds of cash; every pound of heroin yielded 10 pounds of small-denomination bills [3 p. 3].

The emergence of the Bitcoin currency changed the situation dramatically: Bitcoin used together with the anonymity provided by the TOR network enables ordering, delivering and anonymously paying of digital goods and criminal services! For example, the [Figure 2, "Anonymous division of labour in crime"](#) shows a typical hidden service in TOR's dark net offering typical criminal hacker activities. The price is given in Bitcoin.



Product	Price	Quantity
Small Job like Email, Facebook etc hacking	0.451 ₿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	1.128 ₿	1 X Buy now

Figure 2. Anonymous division of labour in crime

Mitigate the Devastating Effects of Crime Economy Through Eradicating Bitcoin

Money flow has always been a critical part in criminal activities. Therefore, it is not a big surprise that criminals welcome and widely use the new payment system. For example, the total sales volume of the Silk Road market place in 2012 is estimated over 1,220 million USD per month which corresponded to 4.5%-9% of all Bitcoin trades [2].

Furthermore, anonymous payment enables organized crime to outsource certain functions. This leads to markets of criminal services founding a - what the author calls - "crime economy" (cf. [Table 1, "Impact of crime on society"](#)).

Table 1. Impact of crime on society

Organisa-tional form	Description	Social impact
<i>Individual criminals</i>	Not cooperating individuals	low
<i>Organized crime</i>	Criminal syndicates, lawless states and army	high
<i>Crime economy</i>	Anonymous global crime markets: Bitcoin + TOR network	huge

Solution

There is a wide consensus that the combination of the TOR-network with the anonymous *Bitcoin* transactions enables and supports the new "global crime economy". But where to put the lever? Should we fight against TOR or Bitcoin or both? What about other crypto currencies, like *Dash*?

In my opinion, we need the TOR network to defend our democracies because TOR's privacy property contributes in maintaining free political opinion forming. Also, the alternative of banning Bitcoin and getting more control over illicit money flow, seems promising: It will very efficiently disrupt essential functions of organized crime.

But is it technically feasible to ban Bitcoin? In our favour is the fact that Bitcoin's (and also Dash's) consensus system - also known as "mining"- is based on the so called *prove of work* mechanism. Indeed, Bitcoin's book-keeping system only trusts the miner who wins a competition game, consisting in resolving a (complete useless) puzzle by brute force: Statistically,

the winner is the miner who is able to waste more computer power and energy than any other competitor. At the same the system attributes him the role of the elected and trusted bookkeeper for the current block-chain block.

The magnitude of this energy waste is tremendous: “The energy used by Bitcoin mining is comparable to Irish national energy consumption” [4], 4]. Besides the environmental impact, certain Bitcoin obfuscation techniques make transactions non-traceable and anonymous. The same also applies to the *Dash* currency with its “PrivateSend” feature.

On the other hand, it is precisely this huge energy waste that makes it easy to identify the few remaining Bitcoin and Dash mining farms ruling the whole system. Thus, a possible solution could be: **Prohibit mining!** It will destabilize Bitcoin’s and Dash’s infrastructure and protect the environment from a huge energy waste! At the same time eradicating Bitcoin it will affect seriously the global crime economy which relies on non-traceable crypto currencies. Anonymous exchange of criminal services will dye out if we manage to disrupt non-traceable money flow.

The suggested solution alone will not have the desired effect, if not not all concerned countries will participate in banning mining. This is why complementary measures like e.g. prohibiting Bitcoin currency exchange should be considered. We should also keep in mind, that regulative measures against Bitcoin (and similar currencies) will only succeed, if we are able to offer an alternative crypto-currency with similar properties to legitimate users. The technology is available: traceable, prove-of-work-free currencies exist and are ready to use [1]. In this regard I am looking forward to Ethereum’s hard fork from *proof of work* to *proof of stake* which is believed to happen in 2017 [6]

References

1. I. Bentov, A. Gabizon, and A. Mizrahi, “Cryptocurrencies without Proof of Work,” *arXiv preprint arXiv:1406.5694*, 2014.
2. N. Christin, “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace,” 2013, pp. 213–224.
3. S. Mihm, “Are Bitcoins the Criminal’s Best Friend?,” *Bloomberg View*, vol. 18, 2013.

Mitigate the Devastating Effects of Crime
Economy Through Eradicating Bitcoin

4. K. J. O'Dwyer and D. Malone, "Bitcoin Mining and Its Energy Footprint," 2013, pp. 280-285.
5. J. Simkin, "Al Capone," *Spartacus Educational*. [\urlhttp://spartacus-educational.com/USAcapone.htm](http://spartacus-educational.com/USAcapone.htm), Nov-2014.
6. V. Zamfir, "Introducing Casper 'the Friendly Ghost'," *Ethereum Blog*. Aug-2015.
7. W. Zhou and S. Piramuthu, "Technology Regulation Policy for Business Ethics: An Example of RFID in Supply Chain Management," *Journal of business ethics*, vol. 116, no. 2, pp. 327-340, 2013.