Mathematical Structures and Modeling
2017. N. 4(44). PP. 136–140

UDC 004.056
DOI: 10.25513/2222-8772.2017.4.136-140

SMART CONTRACTS AND CYBERCRIME: A GAME CHANGER?

L. Brunoni
Scientific collaborator, MLaw, MArts, e-mail: luca.brunoni@he-arc.ch
O. Beaudet-Labrecque
Research Assistant, Criminologist, MAS LCE Institut de lutte contre lacriminalite economique (ILCE), e-mail: olivier.beaudet-labrecque@he-arc.ch

Haute ecole de gestion Arc (HES-SO // Haute ecole de Suisse Occidentale), Neuchatel, Switzerland

Abstract. The purpose of this paper is to provide a brief explanation regarding the authors' current research in the field of the possible uses of smart contracts in cybercrime, focusing in particular on how the technology could provide a substitute for trust both in client-criminal transactions and in transactions taking place within criminal organizations. The authors share the conviction put forward by Alharby and Moorsel [1] in their 2017 analysis of blockchain-based smart contracts that there is a "lack of studies on criminal activities in smart contracts": while quality research does exist, including a paper by Juels et al. [2] detailing three types of such activities that can be facilitated by the technology, it is evident that the subject deserves a more widespread attention. Quality research, in fact, could play an important role in aiding authorities and regulators to understand the issue and react accordingly.

Keywords: smart contracts, blockchain, cybercrime, cybersecurity, criminal behavior.

1. Trust in commercial dealings

From prehistoric barter to online marketplaces, trust has always played an essential role in commercial dealings. In earlier times, people could only rely on instincts and experience when evaluating the reliability of a proposed transaction. The development of the rule of law brought more security, shifting trust from an interpersonal level to a reliance on society and institutions, which had the power to enforce transactions and provide relief to a wronged party. This shift has been essential to the development of commercial relationships as we know them today. A specific commercial field, however, has always remained detached from the conflict resolution mechanisms provided by the state, and remains ruled almost exclusively by interpersonal trust: the illegal market, which today has crossed the border into the cyber world. Dealings conducted within this context require varying levels of trust and reliability from the parties involved: a small-time drug dealer, for example, will not need the same guarantees as a major wholesaler in

order to go through with a deal, because the stakes are radically different. It is worth mentioning, moreover, that criminals active in the illegal marketplace face a double issue: on one side, they are confronted with similar economic constraints as their legal counterparts, and on the other, they are exposed to bigger legal risks.

While a good number of criminals, especially small-time, operate alone, running an illegitimate activity typically requires some level of organization. The business relationships between the members fall outside the scope of legal remedies, and when those would be available (e.g. recovering a debt that is not explicitly related to the illegal activity) they are seldom used, because either of the risk of drawing attention, or of the respect of a code of conduct according to which calling upon the authorities is a serious violation. This means that the element of trust is a paramount factor in the existence of a criminal network. There are other factors that go alongside trust, such as obedience, fear, hierarchy, family relationships, etc., which depend on the type, size, and activity of the organization.

2. Trust in cybercriminal transactions

In the realm of cybercrime, which is the focus of the authors' research, criminal networks are often populated by members who ignore the identity of their partners. Perhaps the most famous example is the organization behind the Silk Road website, a now dismantled dark net marketplace where users could buy and sell any type of illegal goods, including fire arms, drugs and counterfeit documents. The alleged mastermind behind the website, Ross Ulbricht, recruited collaborators online and tasked them with both back-end programming and customer service. Although Ulbricht ignored the real identity of the first collaborators, he later asked new recruits to send him a copy of their ID. Ulbricht, on the other hand, never disclosed his own identity. He paid his collaborators with Bitcoin taken from the revenue of the site. There was reciprocal trust in the sense that Ulbricht trusted them to do their work as requested and the collaborators trusted that he would send the agreed-upon Bitcoin. Eventually, one of these collaborators managed to steal some Bitcoin from the site, and Ulbricht allegedly retaliated by sending a man he contacted online to have the thief beat up and killed. Ulbricht paid a high price for the murder and received photo proof that the deed was done. Yet nobody died: the contract killer was in reality an undercover agent, who staged a fake murder and sent fabricated proof to his client.

3. The problem of trust

The Silk Road example pinpoints several problems that relate to trust and criminal activities in the cyber world. First of all, criminal services available on the dark web, such as the much publicized widespread availability of killers for hire, require a high degree of trust from the customer. Other sales and transactions have a way of auto-regulating themselves, especially because the offeror has a stake in keeping his customers satisfied if he hopes to acquire a reputation and grow his business; this is the case, for example, in the drug market or in the market of

viruses, hacking tools, etc. Still, a certain degree of trust is inherent to every transaction.

At an organizational level, the lack of real-life identities and the reticence criminals on the dark web show with regard to disclosing personal details constitute the main trust-related problems. Obtaining ID might have worked for Ulbricht, but it is not likely to become a standard general practice. Cryptocurrency payments — the obvious choice for transactions in an anonymous, criminal underworld — depend solely on the goodwill of the payer, especially when it comes to compensating a collaborator for his work.

4. Smart contracts

Some of the issues described above could potentially be solved through the integration of smart contracts. Smart contracts are computer programs that run securely on the blockchain; they execute autonomously according to pre-set variables, and the result, verified and inscribed into the blockchain, is virtually irreversible. This ensures that an agreed upon transaction, which typically involves a cryptocurrency transfer, takes place when the conditions set by the parties – and translated into the smart contract's code – are met. In a standard business environment, execution of agreement depends on the goodwill of the parties, and can be enforced through the court system in case of default. Smart contracts automatically enforce the desired outcome of the agreement, thus eliminating the need of trusting and depending on the other party or state authorities once the terms have been agreed.

In a criminal environment, where enforcing a deal through the court system is in general not an option, characteristics of smart contracts could become a valuable asset. The anonymity of the transaction is also guaranteed, which means that the parties can conduct deals without revealing their identities – to each other and to other parties that might observe the transaction, which includes police and prosecution authorities.

The technology could therefore play a role both in client-criminal transactions and in transaction taking place within criminal organizations. In the first case, it could help guaranteeing that both parties get what they want out of the deal, without the need of establishing trust through reputation, disclosing identity, or by making promises that, in a cybercrime environment, have little value. In the second, smart contracts could strengthen a criminal network by ensuring that every party to a criminal enterprise receives the agreed share of a determined cryptocurrency revenue stream.

While these case scenarios are certainly appealing to criminals — and worrisome to state authorities — it must be stressed that smart contracts as a technology are in their beginning phase, and that the realization of such implementations, in order to be functional and versatile enough to suit every transaction's needs, depend on whether several technical challenges can be overcome. These include, in particular, the integrations of oracles (external data feeds that input information triggering the execution of the smart contracts) capable of verifying the successful

executions of criminal transactions, and the difficulty of translating certain types of relationships between criminals in smart contract language. These obstacles are in principle no different than those faced by parties wishing to implement smart contracts for non-illegal transactions. The degree of flexibility provided by the technology simply cannot match that offered by a legal document, and as such, smart contracts are for the moment best suited for executing transactions that lack complexity and nuance.

5. Conclusion

The potential of smart contract technology as an asset in criminal activities and organizations cannot be underestimated. While it is certain that the current lack of flexibility of smart contracts and the many technical challenges to overcome currently limit the above-discussed applications, it is also undoubted that the technology will evolve quickly. It is therefore essential that quality research is conducted in the field and that authorities begin to take notice of the phenomenon, its possible impacts, and to address the issues it could generate with regard to the investigation and prosecution of cybercriminal activities.

References

1. Alhabry M., van Moorsel A. Blockchain-Based Smart Contracts: A Systematic Mapping Study / Proceedings of the 3rd International Conference on Artificial Intelligence and Soft Computing, 2017.
2. Juels A., Kosba A., Shi E. The ring of gyges: Investigating the future of criminal smart contracts / Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

СМАРТ-КОНТРАКТЫ И КИБЕРПРЕСТУПНОСТЬ: ПРАВИЛА ИГРЫ МЕНЯЮТСЯ?

Л. Брунони
научный сотрудник, магистр права, магистр искусств, e-mail: luca.brunoni@he-arc.ch
О. Буде-Лабрек
Помощник по исследованиям, криминолог, магистр программы повышения квалификации по борьбе с экономической преступностью, Институт по борьбе с экономическими преступлениями (ILCE), e-mail: olivier.beaudet-labrecque@he-arc.ch

Высшая школа менеджмента Арк (Университет прикладных наук Западной Швейцарии) Невшатель, Швейцария

Аннотация. Цель данной статьи — дать краткое объяснение текущих исследований авторов в области возможного использования смарт-контрактов в киберпреступлениях, рассказав, в частности, о том, как технология может заменить доверие в транзакциях между клиентом и преступником, а также в транзакциях,

совершаемых внутри преступных организаций. Авторы разделяют убежденность, высказанную Альхарби и Мурселем [1] в 2017 г. в их анализе смарт-контрактов на основе блокчейна, об «отсутствии исследований преступной деятельности в смарт-контрактах»: качественные исследования на самом деле существуют, в частности статья Джуэлса и др. [2], описывающая три вида такой деятельности, которая может быть облегчена технологией, но очевидно, что предмет заслуживает более широкого внимания. Качественные исследования, по сути, могут сыграть важную роль в понимании этого вопроса властями и регулирующими органами, что позволит реагировать соответствующим образом.

Ключевые слова: смарт-контракты, блокчейн, киберпреступность, кибербезопасность, преступное поведение.

Дата поступления в редакцию: 04.11.2017