Blockchain's future role in cybersecurity. Analysis of defensive and offensive potential leveraging blockchain-based platforms

Artur Rot
Dept.of Information Systems
Wrocław University of Economics
Wrocław, Poland
orcid.org/0000-0002-7281-8253

Bartosz Blaicke
Dept.of Information Systems
Wrocław University of Economics
Wrocław, Poland
orcid.org/0000-0002-5083-0059

***Abstract*—*Blockchain and cybersecurity are two current themes in Information Technology that have evolved and gained tremendous attention over the past few years. In this paper authors aim to structure existing and potential use of blockchain-based cybersecurity solutions from the perspective of attackers and defenders to assess whether the intersection will tip the scales in favor of one of these groups. Historically blockchain has been mainly associated with innovative financial services (including crypto-currencies) but it has other emerging use cases within e-government, supply chain management as well as security (e.g. encryption, identity and authentication, data security). On the other hand, blockchain-based platforms are increasingly a target of malicious actors and could be used as an initial attack vector. Therefore, there is a case to be made weather further adoption of blockchain-based solutions should be encouraged or not from a security standpoint and if the overall potential for change could be net positive.*

Keywords*—*blockchain, cybersecurity, cryptography, blockchain-based platforms

I. Introduction

Blockchain technology was introduced in 2008 as a cornerstone of bitcoin [1] that has gained widespread attention as the first crypto-currency. Moreover, starting from mid-2010's users began to realize that blockchain as the foundational technology can have much wider use than the bitcoin itself, and the two terms started to follow separate paths as blockchain began to be adopted for additional use cases [2] and other crypto currencies such as Ethereum were gaining prominence.

In the simplest terms, blockchain (also described as a "digital ledger") is a distributed database constantly reconciling new information (blocks) that are appended onto the end of the dataset, forming a "block-chain" [3]. The data is stored in multiple locations (in contrast to centrally stored databases) therefore being by definition public and widely verifiable thus more difficult to manipulate given that the same copy exists simultaneously in many places.

Blockchain-based technologies such as crypto-currencies have also became prime targets for digital "bank heists" and remained under a steady barrage of attacks as the value of the bitcoin currency increased logarithmically from 30 cents to close to USD 14,000 per bitcoin at the top of the hype [4]. That increase in value lead to multiple attacks including early 2011 attack on Japanese exchange platform Mt. Gox that led to loss of USD 8.75mn and was later followed by one of the largest bitcoin heist of USD 450mn in 2013 [5]. In addition, the exceptional privacy provided by crypto-currencies allowed the ransomware attacks to proliferate as just 35 top ransomware families received more than USD 12mn in payments from victims between 2013 and mid-2017 [6].

However, as described earlier, blockchain is constantly evolving and no longer only restricted to crypto-currencies as new use cases are being brought to life influencing other digital areas. This article is trying to fill the still not well researched intersection of blockchain and security. We will try to better understand blockchain's impact from security point of view by reviewing and structuring direct and indirect influences that technology might have. The additional contribution of this paper is the basic structure and overview of indirect security tools leveraging blockchain concepts that are being introduced and deployed as part of state-of-the-art cybersecurity defenses which has not been yet captured in formal literature.

II. Segmentation framework

To allow for a high-level comparison of the blockchain potential across defensive and offensive areas we introduce a basic framework in Fig. 1 to map all of the solutions.

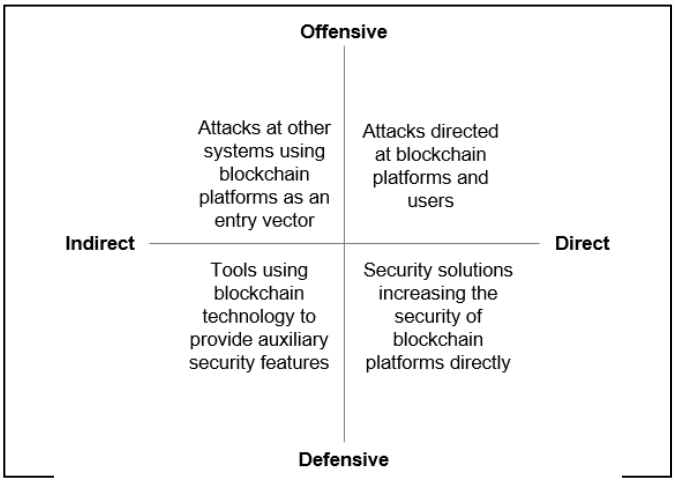

Fig. 1. Framework used to compare blockchain's technology cybersecurity influence across different areas

The first dimension used differentiates between offensive and defensive capabilities. The second one introduces the distinction between solutions that target the blockchain platforms directly in contrast to leveraging blockchain as "a mean to an end". Such approach allows us to divide all the

methods and technologies into four quadrants based on how they place on both dimensions. Fig. 1 provides a brief one sentence overview of each quadrant, with further explanation of the dimensions following in the subsequent chapters.

A. Capabilities dimension

It is possible to look at blockchain from two distinctive perspectives. The first one being an adversary or attacker that is typically trying to exploit, disrupt, modify or broadly hack blockchain-based solutions. These actors have a malicious intent and will employ an array of methods to achieve their means. We would consider these methods to be offensive capabilities.

The second perspective is looking at the issue from the users, platform owners or security professionals' side that are considered here broadly as defenders. These righteous actors can deploy various techniques and solutions to protect their blockchain-based solutions and information assets. Thus, we would consider these to be defensive capabilities.

B. Influence dimension

The influence aspect on the other hand is slightly more complex. First, the direct influence is describing the solutions pool that is affecting the blockchain platforms directly. In other words, if an attack is trying to extract money from the crypto-currency exchange or a solution tries to improve security of the blockchain based smart contracts it would be considered part of the direct influence. On the other hand, when an adversary is using blockchain indirectly to achieve a different goal that will influence other platforms and systems we consider that to be an indirect influence.

III. BLOCKCHAIN-BASED ATTACKS

Detailed look at the attack side reveals that there are more than 30 various attacks and types of vulnerabilities divided into 5 main threat groups that can be used to target blockchain platforms directly [6]. There are however almost no published methodologies or case studies that describe how one can influence other systems or applications through influencing blockchain solution. So far, malicious actors can use Denial of Service (DoS) or look for general vulnerabilities to escalate privileges.

A. Attack types directed at blockchain implementations

There are multiple types of threats that target blockchain and just like with any other technology there are various ways these threats can be executed. There have already been extensive evaluations and overviews of the realm of possible attacks on the blockchain such as [7] that can be summarized into the following:

- Double-spending threats – attackers try to use the same cryptocurrency for multiple transactions for example through quick successive transactions, reversing transactions or sending conflicting pre-mind transactions into the block. In total there are five different attack methods interfering mostly with transaction verification mechanism;
- Mining/pool threats – due to very high difficulty of solo bitcoin mining, miners join pools to combine their computing power and share profits from successful mining. In these scenarios' attackers try to collect more than their fair share of the loot. Overall there are five known types of attacks mostly affecting blockchain consensus mechanism;
- Wallet threats – To store cryptocurrencies and initiate transactions private-key based authentication is used. A wallet in this setup is a collection of private keys to manage all of the transaction and accounts. There are five attacks and bugs that target this authentication mechanism, in many instances using flaws in Elliptic Curve Digital Signature Algorithm (ECDSA);
- Network threats – Being a distributed network there are multiple ways to influence mining nodes and users submitting transactions. In total there are at least 10 different known types of attacks, leveraging flaws in blockchain protocol, internet routing or peer-to-peer network limitations;
- Smart contact threats – Smart contracts are scripts that execute transactions when certain conditions are met. So far these are associated with another major cryptocurrency called Ether (part of Ethereum platform). There are five types of attacks that are executed by exploiting design flaws and vulnerabilities.

The category with most attacks is using network-based elements given the distributed nature of blockchain. However, all of the above described approaches are equally dangerous as means of extracting value from mining pools, customer wallets or smart contracts.

B. Using blockchain to atttack and influence other systems

On the other hand, there are traditional attack vectors that could be used within the blockchain realm to cause further damage to other systems beyond the blockchain platform alone. These would include:

- Distributed Denial of Service (DDoS). While it is harder to unleash a DDoS attack on a blockchain itself due to its' distributed nature and built-in prevention mechanism it is still possible to perform a sophisticated DDoS attack that could affect the entire machine if it is running other services as well.
- Bugs and vulnerabilities. It is also possible to find and exploit vulnerabilities of a blockchain service or software that might be related to a specific implementation or environment on a server or client rather than flaws in the system itself. Such attempt could lead to privilege escalation of the attacker allowing for easier subsequent lateral movements.

Therefore, it appears that it is not easy to target blockchain based solutions as an enabler of a more complex cyberattack or it has not been recognized or documented as one by any of the previous victims. It does not mean it is not possible but most likely it is not widely used yet.

IV. BLOCKCHAIN-BASED DEFENSE

Blockchain has been designed with certain security elements in mind (such a distributed nature of data storage) however there are additional concepts that are being proposed to further increase the potential security. In addition, entrepreneurs and researchers have been expanding on the defense concepts as well and employ some of these mechanism in novel ways in state-of-the-art solutions. Some

have even used blockchain as a basis for drawing up a decentralized security framework [8].

A. Increasing security of blockchains

In order to improve on the original blockchain technology concepts there are emerging suggestions regarding new ways security enhancements could be implemented for the benefit of the miners and the broader community, such as:

- SmartPool – proposal for a different way of handling the mining pool than the existing peer-to-peer approach. The increase in security comes from better management of share (re)submitting in different batches and deployment of the pool as a smart contract [9].
- Quantitative Framework – two-part approach with a blockchain simulator and a security model that creates the parameters for best counterreaction of the blockchain network to double spending and selfish mining attacks [10].
- OYENTE – bug detection method within smart contracts that analyzes the bytecode of smart contracts via symbolic execution in search for flaws in transaction ordering, timestamps, mishandled exceptions and potential reuse of completed contracts [11].
- Hawk – privacy protection mechanism to not store transaction details in "clear text" on blockchains that are used as part of smart contracts without the need to employ additional security layers such as obfuscation, or encryption [12].
- Town Crier – authenticated data feed system for smart contracts that need to obtain trusted data from external sources located outside of that blockchain. It can include stock prices or government provided data among others that can initiate or influence contracts and can use secure credentials for additional access protection layer [13].
- Ledger – a company that manufactures and sells secure software and hardware-based cryptocurrency wallets to store and manage cryptocurrencies including multi authorization on custom operating system BOLOS (Blockchain Open Ledger Operating System) and hardware security elements including externally certified (ANSSI and EAL5+) tamper-resistant chip.

Most of the above suggestions have already been collected in [14] and only OYENTE-style concept has been implemented in a real-life solution as described in the next chapter. It is likely that many of the above will also be incorporated into various blockchain platforms in the near future. However, such commercialization in most cases requires significant time and resources to scale and be widely adopted.

B. New security tools leveraging blockchain technology

Blockchain concepts have also been applied in solutions that aid defenders in securing their existing environments. There are multiple start-ups and published methodologies that employ basic blockchain concepts to achieve different functionalities such as improved authentication, better data protection mechanism or holistic cybersecurity platforms. We group these solutions into several types based on core functionality, providing names of relevant companies and describing one to present an overview of what they offer and how does it leverage blockchain technology:

- Digital identity (e.g. Cambridge Blockchain, Civic, Evernym, GemOS, NuID, ShoCard). Civic is an example of an online biometrics-based ID platform. It envisions a broad set of use cases where all personal information including social, financial and medical files are stored and shared via blockchain on "as needed" basis. It allows to maintain full control by the owner through use of specific consents required for any type of data sharing. Cambridge Blockchain adds a layer of compliance to a similar digital identity platform that simultaniously helps companies prove compliance with the European General Data Protection Regulation (GDPR) and other financial regulations.
- Authentication and access management (e.g. REMME, NuCypher, Nuggets). REMME is an example of blockchain based authentication assigning each device a specific SSL (Secure Socket Layer) certificate that is then stored within a private blockchain instead of using passwords for authentication. Therefore, hackers cannot easily forge certificates to obtain access and since it allows for a one-click login it prevents most common attacks that rely on human factor such as key loggers, brute force password guessing or some forms of phishing. Nuggets on the other hand is focused strictly on eCommerce use cases while providing purchase history encrypted into a blockchain.
- Security platforms (e.g. Block Armour, Guardtime). Guardtime offers a full blockchain based technology stack ranging from backend database management, through middleware to secure transaction handling. The company expanded on the linked timestamp concept that is used in blockchain as the proof of work as well as within smart contracts. In addition, over the years the company added innovations such as attribution of origin for tracking advertising, tamper transparent software or post-quantum signatures as well as anti-tamper hardware solutions to their solution portfolio. Block Armour on the other hand developed a different approach called Blockchain Defined Perimeter (BDP) deploying a zero-trust architecture. It renders critical systems difficult to discover and thus not being targeted for attacks while providing a secure communication channel for legitimate users.
- Privacy management (e.g. MindSafe, Obsidian). Obsidian offers messaging meta-data privacy protection by using blockchain to scatter meta-data throughout the distributed ledger. It was created as a response to issues with existing end-to-end-encryption messengers such as Facebook Messenger or WhatsApp that provide encryption for the communications content but still leave significant metadata behind (as well as full access by corporate owners). MindSafe tries to go one step further and is developing an entire anonymized and decentralized

network using blockchain architecture to communicate and share files securely.

- DDoS protection (e.g. Gladius, Nebulis). Nebulis envisioned the use of Ethereum blockchain to provide an alternative infrastructure to the Domain Name System (DNS) that is currently used to translate Internet Protocol (IP) addresses into human-readable Uniform Resource Locators (URLs). However, its current status is unknown suggesting this solution did not manage to scale commercially. Gladius picked up on the concept and created a solution addressing the same issue. The company proposed to use blockchain to create a distributed version of the traditional Content Delivery Network (CDN) and Web Application Firewall (WAF) systems that can redirect and better handle potentially overwhelming flows of data or requests.

- Data management (e.g. Datum, Gospel Technology). Gospel has developed a private blockchain (Gospel Trusted Data Network) that provides full control over data sharing through contextual data access and additional connectors for bulk data exchange with existing applications. Datum is combining the blockchain with smart contract by offering a decentralized marketplace for social and IoT data. In other words it enables optional selling and buying of stored data while enforcing data usage rules as set by the data owner who uploaded the data on the platform.

- IoT security (e.g. xage security). Xage is a blockchain enabled security platform designed for industrial Internet of Things environments. It uses the decentralized consensus mechanism from blockchain systems to identify and isolate bad devices and applications. For example when a new devices is connected to the existing environment the consensus is used to validate its purpose or if it is rouge, prevent it from any further communication by exclusion. Therefore, it can be considered as a self-healing mechanism that automatically adapts the enforcement of security policies directly on each edge device enabling better control of users and applications at most granular level.

- Vulnerability management (e.g. Synthetic Minds). Synthetic Minds envisions a safer blockchain code by automating the analysis and synthesis of the smart contracts code so that it doesn't have bugs and vulnerabilities. While it doesn't focus on the exact four elements that OYENTE approach has proposed, it offers another way to implement a variety of similar concept from academic research into a real-life scenario. In addition, the advertised capability to create safe and secure smart contracts through "auto-coding" and then simulation of the contract behavior will expand the portfolio of available preventive tools and allow non-technical users to take advantage of these next generation capabilities.

These 20 companies clearly show that there are multiple use cases that are already being pursued through use of blockchains in new and innovative ways. Currently, the closest fit for broader adoption of blockchain based solutions within security are identity and access management tools that represent 45% of the identified companies. However, many firms have shown that is not only possible to address other significant issues such as DDoS protection or data management but also create a portfolio of solutions and services (or a technology stack) that could be used within many different layers of security infrastructure offering a new way to design defense perimeter elements.

V. Conclusions

Despite being a relatively young technology with only 11 years since inception, blockchain has gained significant attention and headlines across the world. Blockchain technology is attractive due to some of its special properties. As described in the paper, there were multiple attacks that target the blockchain itself. So far, most of these were aimed to steal crypto-currency or extort money in ransomware schemes. On the other end of the spectrum, there are some emerging security improvement proposals that have the potential to improve protection of the core elements within various blockchain implementations and even influence other areas. However, since hardly any have been commercially implemented the attackers are in the lead when it comes to direct offensive and defensive battle for blockchain.

However, on the indirect side, there are hardly any existing cases that can show leveraging blockchain to affect security of other systems can be done successfully at scale. It does not mean that there are no "zero-day" vulnerabilities that could be used but they have not been discussed yet or used in a publicly described attack. Moreover, entrepreneurs are building new cybersecurity solutions that leverage blockchain concepts to solve existing problems. The pool of tools available for defenders has already been expanded with solutions answering pain points within digital identity, authentication, privacy, DDoS protection, privacy, IoT security and vulnerability management. All of these are tipping the scale towards a positive influence overall in the indirect area as they are commercially available, and many can be implemented as "add-ons" to the existing infrastructure without the need for costly and time-consuming architecture transformations efforts. However, while they hold strong promise to be effective for single organizations, it will take significant amount of time to reach industry wide deployment scale like other well-established technologies (e.g. firewalls).

Therefore, we believe that overall blockchain as a technology should provide a net positive security effect at the industry level. That should hold true even if the adoption of the technology is higher among malicious rather than righteous actors. It is due to the higher potential of indirect defense solutions and their breadth compared to possible attack vectors that can influence the blockchain itself. Further increase in scale of defense deployments can potentially have additional benefits as increase adoption will have scale effects.

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", 2008. Available: https://bitcoin.org/bitcoin.pdf [Accessed Feb 15, 2019].

[2] B. Marr, "A very brief history of blockchain technology everyone should read", Forbes, 16 Feb 2018. Available: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#19c60b067bc4 [Accessed Feb 15, 2019].

[3] H. Dikariev, M. Miłosz, “Blockchain technology and its applications” (In Polish), Journal of Computer Sciences Institute (JCSI) no. 6 (2018), Lublin, 2018, p. 59-61.

[4] Cryptonite, “Is it too late to invest in Bitcoin? is it just a bubble?”, Hacker Noon, Sept 19, 2018. Available: https://hackernoon.com/is-it-too-late-to-invest-in-bitcoin-is-it-just-a-bubble-704ba4f69d9d [Accessed Feb 17, 2019].

[5] “Bitcoin burglaries: the 5 biggest cryptocurrency heists in history” , Big Think, 23 Aug 2018. Available: https://bigthink.com/reuben-jackson/bitcoin-burglaries-the-5-biggest-cryptocurrency-heists-in-history [Accessed Feb 11, 2019].

[6] M. Paquet-Clouston, B. Haslhofer, B. Dupont, “Ransomware payments in the bitcoin ecosystem”, 2018.

[7] J. H. Mosakheil, "Security threats classification in blockchains", Culminating Projects in Information Assurance. 48, St. Cloud State University, 2018. Available: http://repository.stcloudstate.edu/msia_etds/48 [Accessed Feb 15, 2019].

[8] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework”, 2018.

[9] L. Luu, Y. Velner, J. Teutsch, P. Saxena, “Smart pool: practical decentralized pooled mining”, USENIX Security Symposium, 2017.

[10] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, S. Capkun, “On the security and performance of proof of work blockchains”, ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3-16.

[11] L. Luu, D. Chu, H. Olickel, P. Saxena, A. Hobor, “Making Smart Contracts Smarter”, 2016. Available: https://loiluu.com/papers/oyente.pdf [Accessed Feb 19, 2019].

[12] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”, IEEE Symposium on Security and Privacy, 2016, pp. 839-858.

[13] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, “Town crier: An authenticated data feed for smart contracts”, Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270-282.

[14] X. Lia, P. Jianga, T. Chenb, X. Luoa, Q Wenc., “A Survey on the Security of Blockchain Systems”, 2018.