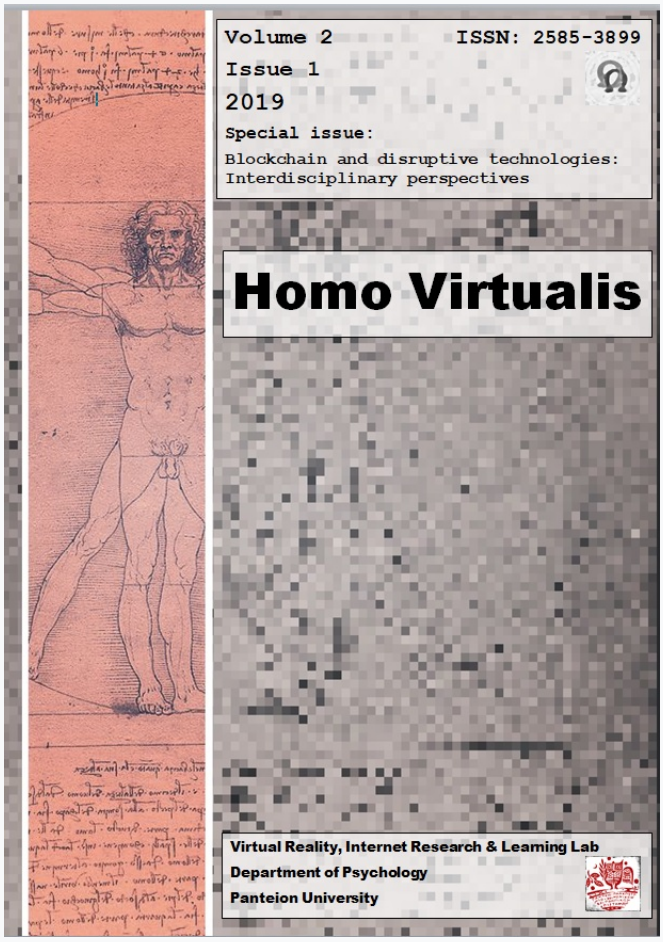
Homo Virtualis

Vol 2, No 1 (2019)

Blockchain and disruptive technologies in social sciences: Interdisciplinary perspectives



Blockchain technologies for leveraging security and privacy

Costas Vassilakis

doi: 10.12681/homvir.20188

To cite this article:

Vassilakis, C. (2019). Blockchain technologies for leveraging security and privacy. *Homo Virtualis*, *2*(1), 7–14. https://doi.org/10.12681/homvir.20188

Homo Virtualis 2(1): 7-14, 2019
ISSN 2585-3899 ∫ doi.org/10.12681/homvir.20188

Blockchain technologies for leveraging security and privacy

Costas Vassilakis[1]

Abstract: The contemporary internet has developed into a complex ecosystem involving humans, services, applications, machines and applications that interact exchanging information, ranging from e-mail messages and social media content to crowdsourcing data and videoconferencing. In this context, a number of security threats such as viruses and malware exist, while additionally the users' privacy is jeopardized by threats such as personal data leakage, usage pattern monitoring, and so forth. The IoT trend renders the Internet ecosystem even more complex, by adding a rich set of services, applications and machines, many of them backed by new user roles; these elements are weaved into everyday life and industry alike. This increases both the number of opportunities available to threat agents for exploitation and the volume and value of the underlying infrastructure and data, increasing thus the user risk level. In this paper, we explore how the Blockchain technology can be used to leverage security and privacy in the modern Internet, both by providing underpinnings for preventive measures and by facilitating digital forensic evidence collection storage, safeguarding and controlled access.

Keywords: *blockchain, privacy, security, internet of things*

[1] Professor, Department of Informatics and Telecommunications, University of the Peloponnese, Greece, costas@uop.gr, Akadimaikou G.K. Vlachou, Tripolis, 22100, Greece.

Homo Virtualis 2(1): 7-14, 2019
ISSN 2585-3899 ∫ doi.org/10.12681/homvir.20188

Τεχνολογίες blockchain για ενίσχυση της ασφάλειας και της ιδιωτικότητας

Κώστας Βασιλάκης[1]

Περίληψη: Το σύγχρονο διαδίκτυο έχει εξελιχθεί σε ένα πολύπλοκο οικοσύστημα που περιλαμβάνει ανθρώπους, υπηρεσίες, συσκευές και εφαρμογές που αλληλεπιδρούν ανταλλάσσοντας πληροφορίες, οι οποίες ποικίλουν από μηνύματα ηλεκτρονικού ταχυδρομείου και περιεχόμενο κοινωνικής δικτύωσης έως δεδομένα πληθοπορισμού και βιντεοδιασκέψεις. Σε αυτό το πλαίσιο εμφανίζεται ένα πλήθος από απειλές στην ασφάλεια όπως οι ιοί και το κακόβουλο λογισμικό, ενώ παράλληλα διακυβεύεται η ιδιωτικότητα των χρηστών από απειλές όπως η διαρροή προσωπικών δεδομένων, η εξαγωγή μοτίβων χρήσης κ.ο.κ. Η τάση του Διαδικτύου των Πραγμάτων (IoT) καθιστά το οικοσύστημα του διαδικτύου ακόμη πιο πολύπλοκο, προσθέτοντας ένα ευρύ σύνολο υπηρεσιών, εφαρμογών και συσκευών, πολλές από τις οποίες υποστηρίζονται από νέους ρόλους χρηστών, και οι οποίες έχουν ενσωματωθεί τόσο στην καθημερινή ζωή όσο και στη βιομηχανία. Αυτή η εξέλιξη πολλαπλασιάζει το πλήθος των ευκαιριών που είναι διαθέσιμες για εκμετάλλευση στους επιτιθέμενους, καθώς και τον όγκο και την αξία των δεδομένων, αυξάνοντας έτσι τον συνολικό βαθμό κινδύνου για τους εμπλεκόμενους χρήστες. Στην παρούσα εργασία διερευνούμε το πώς η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την επαύξηση της ασφάλειας και της ιδιωτικότητας στο μοντέρνο διαδίκτυο, παρέχοντας το υπόβαθρο για προληπτικά μέτρα, καθώς και διευκολύνοντας τη συλλογή, διασφάλιση και ελεγχόμενη πρόσβαση σε ψηφιακά εγκληματολογικά στοιχεία.

Λέξεις-κλειδιά: *blockchain, ασφάλεια, ιδιωτικότητα, διαδίκτυο των πραγμάτων*

Introduction: Contemporary internet and related threats

The contemporary internet has developed into a complex ecosystem involving humans, services, applications, machines and applications that interact exchanging information. The type and value of this information depends on the nature of the application that is involved in the current activities, and may range from e-mail messages and social media content to crowdsourcing data, health-related data and videoconferencing. The hardware, software and data involved in this context constitutes *assets*, with each asset having a *value* for its

[1] Καθηγητής, Τμήμα Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Πελοποννήσου, costas@uop.gr, Ακαδημαϊκού Γ.Κ. Βλάχου, 22100, Τρίπολη

owner and users (ENISA, 2019). For each asset, a number of security threats exist which may demote the value of the assets: these threats are realized through unauthorized access, destruction, disclosure, modification of data, and/or denial of service (ENISA, 2019). Many threats entail also issues for user privacy, including personal data leakage, extraction of patterns of behavior, and so forth.

Recently, the Internet of Things (IoT) has emerged (Gubbi et al., 2013), adding a rich set of services, applications and machines, which are weaved into everyday life and industry alike. Predominant examples of devices used in the user's everyday life are smartphones, tables and wearable computing devices (e.g. smartwatches), while in the domain of industry the Fourth Industrial Revolution covers concepts such as trends of automation, scaling and data exchange in manufacturing technologies (Tsekeris, 2018). This set of services increases the exposed attack surface, i.e. the actions externally visible to the system's users together with the system resources (Manadhata & Wing, 2011). As Manadhata & Wing (2011) note, the more exposed the attack surface, the more likely the system could be successfully attacked, and hence the more insecure it is. Together with the expansion of the attack surface, the IoT renders easily accessible new types of personal data, significantly increasing the threat level to user privacy: for instance, smartwatches collect and transfer heart rates; security cameras capture the interior of homes; smartphones can convey the user location: any compromise of these devices or the relevant data transfers would make these data (which include sensitive data) accessible to attackers. The new level of risk can be conceived by considering that the number of IoT devices with Internet connection in the forthcoming years is expected to become equal to approximately twice the number of non-IoT devices (cf. Figure 1), in combination with the fact that the hardware, firmware and software of IoT devices is not well-engineered in terms of security, since the average IoT device has 25 security flaws many of which are considered to be serious threats to device security and user privacy (HP, 2014). We note here that a compromised device can be exploited by attackers as a standpoint for launching new attacks: this constitutes a significant threat to the operation of the network as a whole (e.g. the Mirai Botnet orchestrated over IoT devices has proven to be related to the most disruptive distributed denial of service (DDoS) attacks (CloudFlare, 2017)), while a device owner could also face legal consequences if her devices were used for attacking other users' infrastructure.

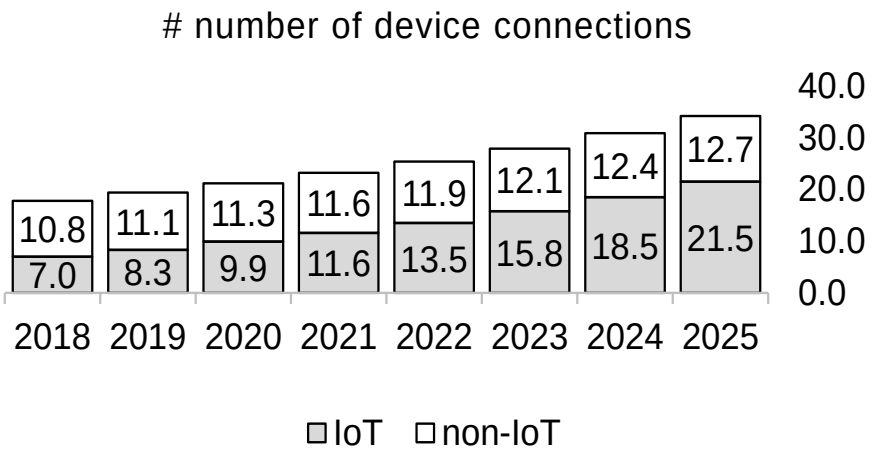


Figure 1. *Projected increase of number of IoT devices (IoT Analytics, 2018)*

In this paper, we explore how the blockchain technology can be used to leverage security and privacy in the modern Internet, both by providing underpinnings for preventive measures and by facilitating digital forensic evidence collection storage, safeguarding and controlled access.

Goal, elements and outline of the blockchain technology

The Blockchain technology has its roots at the first ever decentralized cryptocurrency which was termed "bitcoin" (Barber et al., 2012; Grinberg, 2012). Prior solutions required the existence of a single trusted party to guarantee for the validity, authenticity and notarization of transactions; however this requirement introduced a series of issues, and most notably (Puthal et al., 2018):

1. The trusted party may become rogue and therefore incapable of operating as a trusted party.
2. The trusted party may become compromised and therefore intruders get access to all the data and/or shut off its operation. In this respect, the trusted party constitutes a single point of failure.
3. Usage of a single trusted party is prone to bottlenecks; peer-to-peer communication may alleviate this problem.
4. It may be possible that the trusted party cannot be actually trusted to guarantee the authenticity and validity of all transactions, e.g. for reasons of conflict of interest.

Blockchain operates in a distributed fashion, with all participants assuming part of the responsibility of ascertaining the authenticity, validity and persistence of transactions. It is based on the following basic pillars (Cachin, 2018):

- *Distribution and replication*: the ledger is distributed among the participants of the blockchain system, and each of the participants maintains its own copy. Copies are append-only, contain the whole transaction history and the Blockchain protocol guarantees that past entries cannot be modified or tampered with.
- *Cryptography*: the integrity of the ledger and the privacy and authenticity of transactions as guaranteed through cryptographic techniques. Appropriate cryptographic techniques are also used to provide strong identity guarantees for participants.
- *Consensus:* The transactions, as well as each "block" of information recorded in the blockchain are validated using a consensus mechanism. Effectively, the majority of nodes decides (in cases of disagreement) on which is the version that should be accepted and stored in the blockchain. As noted in (Kolokotronis, 2018), transactions of honest nodes will be included into honest players' blockchains and honest nodes will also agree upon a common prefix of the blockchain.
- *Business logic*: the ledger integrates the business logic that must be executed in the context of transactions; this makes storage of information inseparable from the relevant business aspects and business-level validations.

The basic flow of a blockchain transaction constitutes of the following steps:

- A transaction request is submitted

- The transaction is sent to a peer network
- The network validates the transaction and the user status using known algorithms
- The validated transaction is combined with other transactions and creates a new data block
- The new block is attached to an existing blockchain in a persistent and immutable fashion

Figure 2 illustrates this flow.

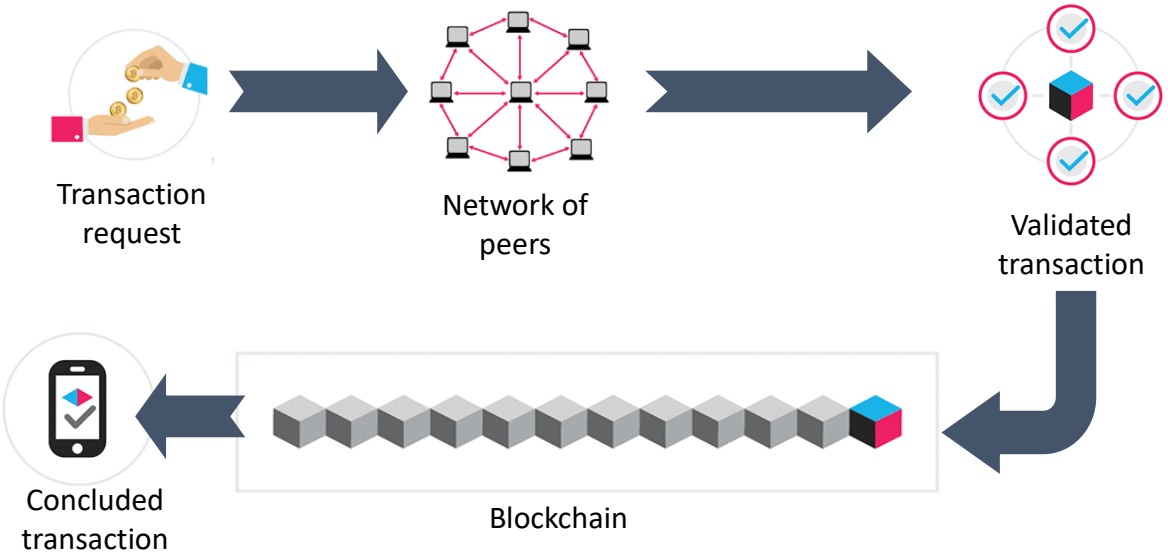


Figure 2. *Basic flow of a blockchain transaction*

Employing blockchain technologies for leveraging security and privacy

In this section we outline opportunities for exploiting blockchain technologies in the context of improving security and user privacy, especially in the presence of IoT devices:

- *Registration of legitimate IoT devices*: users, upon purchase and installation of a new device in their premises (smart homes; industries; offices; etc.) carry out a special procedure to register the device as being known and legitimate. The registration action and related information for the device are stored in a blockchain, and is subsequently exploited by specialized software to distinguish between activities carried out by legitimate and illegitimate/rogue devices. This software may be intrusion detection or intrusion prevention systems (IDS/IPS) (Scarfone & Mell, 2012), which will defend the installation against malicious activities.
- *Identification and recording of security concerns and vulnerabilities*: Specialized software can detect the security issues and vulnerabilities associated with legitimate devices in user premises. This information can then be extracted and used to determine the probability that a device has been compromised (devices with more vul-

nerabilities are more probable to be compromised) and hence the level of trust that should be assigned to this device. Devices with low level of trust will be impeded to perform certain activities within the system, especially ones involving high risk.

- *Underpinnings for device integrity verification*. Checksums (typically cryptographic hashes) of the legitimate devices' firmware, operating system files and configuration files can be computed at a stage that they are known to be clean (non-infected); at later time points, the process can be repeated and newly computed checksums can be compared with those stored in the blockchain. Should discrepancies be identified, the devices are flagged to have been tampered with and device owners are alerted.
- *Maintenance of an update, service or reconfiguration record of the devices*. When a device is updated, serviced or reconfigured, a new record is stored in the blockchain containing information about the procedure carried out (who, when, what). Upon firmware update, operating system update or reconfiguration of the device, the checksum computation procedure mentioned in the previous item is also repeated. The blockchain can also be used to store and access checksums of update files (i.e. firmware update files or operating system patch files), to allow for verification of their authenticity and integrity and avoid the use of infected update files.
- *Recording of forensic evidence for further exploitation*. When traces of attack or breach are identified, these can be securely stored in the blockchain: the secure timestamping and the immutable past properties of the blockchain will leverage the proofing value of this evidence before authorities.

It has to be noted here that the above listed information stored in the blockchain may convey personal data or be otherwise needed to be kept private, since e.g. publishing which vulnerabilities are present at a device can lead adversaries to launch more effective attacks. This issue can be tackled, by arranging that personal, sensitive or otherwise non-disclosable information is stored in the blockchain in an encrypted form, and henceforth only parties holding the decryption keys would be able to effectively access the information.

Conclusions

In the modern Internet multiple threats exist for security and user privacy exist, which are aggrieved by the IoT trend. The blockchain technology can offer the underpinnings to build mechanisms for alleviating these concerns, both at prevention level and at digital forensic maintenance and access level. A number of such directions have been identified in this paper.

It has to be noted here that while the blockchain technology is complex, its use need not be: appropriately build tools and utilities can arrange for a user-friendly way to access blockchain functionalities and blockchain-supported processes that enhance security and privacy. Furthermore, the creation and maintenance of the blockchain infrastructure and related tools may be delegated to providers, in the same way that ISPs arrange for the provision of internet services: under this model, users will only have to subscribe to a provider and thereafter receive services realizing enhanced levels of security.

Acknowledgment

This work was supported by CYBER-TRUST project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 786698.

References

Barber, S., Boyen, X., Shi, E. & Uzun, E. (2012). *Bitter to better -- How to make bitcoin a better currency*. Proceedings of the International Conference on Financial Cryptography and Data Security, 399-414.

Cachin, C. (2018). *Distributing trust with blockchains*. Retrieved March 1, 2019 from https://cachin.com/cc/talks/20180705-blockchain-cern.pdf.

CloudFlare (2017). *What is the Mirai Botnet?* Retrieved 1 March 2019 from https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/.

ENISA (2019). *Risk Management Glossary*. Retrieved 1 March 2019 from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.

Grinberg, R. (2012). Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & *Technology Law Journal*, *4*, 159-208.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29* (7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

HP (2014). *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*. Retrieved 1 March 2019 from https://www8.hp.com/in/en/hp-news/press-release.html?id=1744676.

IoT analytics (2018). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. Retrieved March 2 from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

Kolokotronis N. (2018). *Distributed Ledger Technologies for Enhanced Security & Privacy in the IoT*. Decentralized 2018, November 14-16, 2018 (Athens, Greece). Retrieved 2 March 2019 from https://www.decentralized.com/blog/2018/12/19/decentralized-2018-day-2-nicholas-kolokotronis-university-of-peloponnese/.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos E., &Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine*, *7* (4), 6-14, July 2018.

Scarfone, K. & Mell, P. (2012). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST publication SP 800-94 Rev. 1, Retrieved 2 March from https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft.

Tsekeris, C. (2018). Industry 4.0 and the digitalisation of society: Curse or cure? *Homo Virtualis*, *1* (1), 4-12. doi:http://dx.doi.org/10.12681/homvir.18622

Manadhata, P. K. & Wing, J. M. (2011). An Attack Surface Metric. *IEEE Transactions on Software Engineering*, 37 (3), 371-386, May-June 2011, doi: 10.1109/TSE.2010.60

Notes on Contributor

Costas Vassilakis: Professor at the Department of Informatics and Telecommunications, University of Peloponnese. He holds a degree in Informatics from the University of Athens and a PhD in Informatics from the same university. He has published over 150 papers in international scientific journals and conferences and has participated in more than 30 European and national research and development projects, including CYBER-TRUST, CROSSCULT, TripMentor, Experimedia Blue, e-Tourism, Quality Assurance System for the University of the Peloponnese. He has served a PC member and referee in several international journals and conferences. His research interests include information systems, information security, vulnerability analysis and assessment, software/coding security, distributed systems, service-oriented architectures, semantic web technologies and applications, and personal information management and personalization.