Secured by blockchain: safeguarding Internet of Things devices

Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles and Romain Griffiths

***Abstract*—Blockchain is a disruptive technology that has been widely characterised to be the next big thing. Regardless whether the expectations will be met, the technology has already gained a broad recognition by experts in diverse fields, due to its envisaged profound applications in many sectors and industries, including consumer electronics. Undoubtedly, blockchain may lead to new business models with far-reaching economic impact. In this paper, we consider possible use cases and applications of the blockchain for the consumer electronics industry, and its interplay with the Internet of things. Instead of discussing how the blockchain can revolutionise the supply chain, which has been the main subject of numerous position articles and technical releases, we focus on how it could be employed for enhancing the security of networked consumer devices in a cryptographically verifiable manner. This work is motivated by the large number of recent attacks (sign of a growing trend) that use easily hackable devices as a weaponry for conducting cyber-criminal activities, including the stealing of sensitive personal information. Toward this direction, privacy and data protection aspects of blockchain solutions are also presented and linked to regulatory framework provisions. Information on already existing blockchain solutions to use is also provided.**

I. Introduction

THE vision of the *Internet of things* (IoT) is to establish a whole new ecosystem that is comprised of heterogeneous connected devices communicating to deliver environments that make the way we do business, communicate, and live far more intelligent [5]. In the following years, almost anything in the surrounding environment will be interconnected with billions of other devices, as part of a network of networks. Examples of such IoT devices include sensors and embedded devices in buildings, transportation systems, industrial control systems, etc., as well as, *consumer electronics* (CE) devices, like digital cameras, TVs, computers, and smartphones [18].

The technological and industrial revolution that is brought by the IoT across many sectors and industries would be greatly amplified if it is further combined with blockchain solutions [1], [4]. The blockchain, which is the distributed data structure underlying the Bitcoin, provides a verifiable process for storing transactions or digital assets, on an immutable shared ledger, in a way that it is secure, robust (resistant to node failures), and transparent (*see* Fig. 1); every transaction is accompanied by an auditable proof that is valid and has been accepted and mutually agreed by the nodes. The adoption of the blockchain, or *distributed ledger technology* (DLT), in IoT would lead to powerful systems, allowing IoT devices to act autonomously and execute transactions via smart contracts [7]. Thus, beyond its use in cryptocurrencies, the blockchain has the potential to also impact other industries, including healthcare, retail, and CE [10]. In fact, nearly 2/3 of the aforementioned industries are expected to already have blockchain-based solutions in full production by 2020 [7].

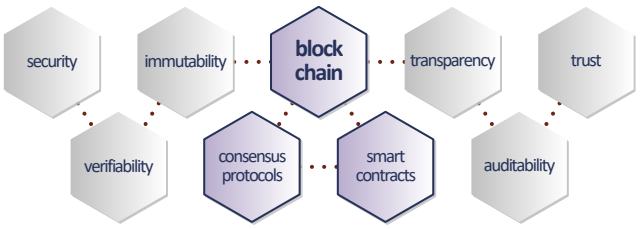

Fig. 1. Notable advantages of the blockchain/distributed ledger technology.

The above technological evolution comes with new forms of threats or attacks that exploit the complexity and heterogeneity of IoT networks, therefore rendering security amongst the most important aspects of a networked world [11]. The fact that the number of intelligent things attributed to, or associated with, the CE industry has greatly increased in the last few years, and will continue to do so, amplifies concerns about the security of networked devices, applications, and services. These often constitute the target of attackers, since they may easily exploit well-known vulnerabilities to accomplish their objectives, e.g. gain unauthorised access to the CE device, take full control of its applications, steal owner's sensitive personal data, deny services to legitimate users, and use it as a vehicle to launch other advanced network attacks. Thus, there is an urgent need for securing the communications among untrusted devices to allow them establish trust and operate transparently.

In this paper, we investigate whether the blockchain could be used for enhancing the security of IoT-enabled CE devices in a cryptographically verifiable manner, along with possible ways for this to be achieved. The fact that the blockchain is a promising approach for increasing security and privacy in the IoT, and the distributed network of its ecosystem, has recently been recognised [9]. The blockchain could define the framework for providing trusted transaction processing and coordination between IoT devices, while ensuring privacy [7]; most importantly, this can be achieved without the presence of a *trusted third party* (TTP) or even the assumption that the devices mutually trust each other. This new paradigm, driven by the blockchain, could bring the transparency and auditing necessary for trusting online services. Although both academia and industry have been extensively exploring the blockchain and its potential applications, the area of using blockchain for strengthening the IoT security and privacy, or for addressing cyber-security needs in general, is still in its infancy. A lot of grand challenges remain to be tackled, including processing power, storage, and scalability, which are relevant (and critical) for the application of blockchain-based solutions to IoT. The fact that data stored on the blockchain cannot be changed and

are visible to all the participants, raises even more challenges; these are the need for long-term security, data confidentiality, and the right to be forgotten in blockchain applications.

II. How the Blockchain Works

The blockchain was introduced with the Bitcoin as part of the solution that aims at tackling, in a distributed fashion, the double-spending problem in a trustless network of peer nodes; it is also referred to as the Bitcoin's backbone protocol. The proposed solution heavily relies on cryptographic mechanisms, ensuring the immutability —among other things— of the data stored on the distributed ledger; moreover, a "security through transparency" approach is taken, according to which all nodes' transactions are publicly announced, hence allowing anyone to verify their validity. The transactions are digitally signed with the *private key* of the asset's (i.e. coin's in the case of Bitcoin) owner, and therefore their authenticity is verified by using his *public key* that has been included in the blockchain. A number of new transactions is packed into a block, containing links to transactions that already appear in the blockchain (creating a chain of blocks), and is subsequently appended to the structure. The maintenance of the ledger, that is, the validation of new transactions, their aggregation into blocks, and their chaining with the structure, is carried out by the class of network nodes called *miners*. The mutual agreement on the validity (or not) of the newly created block is performed according to a *consensus* protocol. The miners also ensure that tampering, or removal, of the blocks in the ledger is impossible, therefore making the whole data structure immutable. In Bitcoin, the miners get new coins as a reward for creating blocks and supporting the network. This functions as an incentive for the miners to stay honest by adhering to the protocol specifications.

Blockchain and IoT considerations

The design of a blockchain solution for securing IoT devices and their transactions is not straightforward. In most cases, an IoT device's available resources are highly constrained, whilst there is a need for performing transactions at high speed. These requirements call for efficient blockchain solutions; key design factors that determine both their security and performance, in the context of the IoT, are briefly presented below.

Modelling: Depending on whether the ledger is open to the public, i.e. it can be used by all network nodes, it is classified as public or private (*see* Fig. 2). Moreover, if the miners that maintain the ledger have been selected a priori, then the ledger is called permissioned; otherwise, if any node can be a miner, the ledger is said to be unpermissioned.

In an IoT security scenario, the blockchain that should be designed needs not necessarily be universal; in fact, there may be many local and global blockchains with different purposes; the use of sidechains could also prove to be efficient in certain cases. The model to be used in each case depends on security, scalability, performance, and other critical for the IoT scenario requirements. There are trade-offs between the above criteria: a private blockchain with less users could minimise the integrity verification time and enjoy almost immediate tamper resistance and detection; on the other hand, this choice reduce security, since we rely on less nodes to maintain the data structure.

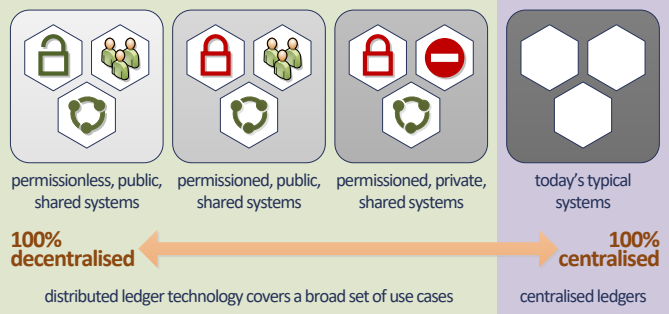

Fig. 2. Variation of different ledger technologies in the centralisation degree.

Consensus: There exist many consensus protocols that are used by blockchain-based applications. Their objective is to allow the nodes of the network agree on a *single* version of valid transactions. Primary examples include the following:

- The *proof of work* (PoW) consensus is used by Bitcoin and Ethereum. The miners have to spend a large amount of processing power so as to solve a hard computational problem (a block's hash value must have a certain number of leading zeros) and create a new transactions' block.
- The *proof of stake* (PoS) is likely to be used by Ethereum. In this case, the node to create the next block in the ledger (and hence maintain its security) is decided according to the percentage of coins (state) within the system.
- The *proof of elapsed time* (PoET) has been incorporated in Intel's Sawtooth Lake. The protocol depends on a fair leader election process, realised in a trusted module, for deciding who should extend the ledger; such modules are available for IoT-enabled CE devices.
- The *Ripple consensus protocol* is another example, as it has resiliency against adversarial faults —these have been deliberately chosen to maximally harm the protocol; such protocols are called *Byzantine fault tolerant* (BFT).

The processing power that PoW consensus algorithms require to be devoted can be adjusted to the application needs in order to meet performance requirements. It is clear that lowering the hardness of the computational puzzle to solve also impacts the security offered by the application. Hence, an optimal balance should be found if PoW is to be used in blockchain-based IoT applications where the speed at which the transactions can be processed is an important choice factor.

Smart contracts: These are computer scripts that are stored in, and are automatically executed by, a distributed ledger once they are triggered [4]. They are written in a protocol-specific programming language, e.g. C++, Java, Python, etc., and they allow nodes to enjoy increased automation when creating and executing a contract. They are an important part of blockchain-based IoT applications, where the IoT devices are expected to be highly autonomous (take the context of machine-to-machine communications as an example) and transact with each other based on some predefined criteria [15].

III. Need for Securing IoT-enabled CE Devices

Security and privacy are increasingly important factors for the acceptance of IoT products and services by consumers and

end-users respectively. However, as the networked CE devices become ubiquitous, the task of ensuring their security becomes increasingly difficult, since attacks get more frequent and even more sophisticated. There are many recent examples of attacks exploiting IoT-enabled CE appliances, like smart televisions, refrigerators, and cameras, to perform *denial of service* (DoS) and *distributed DoS* (DDoS) attacks, to spy on people in their homes/offices, and hijack communication links, delivering full control of anything that is remotely accessible and controlled to an attacker. Recent reports indicate that DDoS, cloud-based, and mobile attacks are among the most common attacks [17]. The availability of botnets-for-hire has led to the noticeable increase in DDoS attacks and it is highly likely to see that the IoT will further facilitate the formation of such botnet armies. A recent example of DDoS attack in Oct. 2016, attributed to Mirai botnet, affected millions of users and companies, also crippling the servers of popular services, like Twitter, Netflix, and PayPal; this simple malware infected the IoT devices that used default settings and credentials.

Most of the security issues arise from devices with flawed design or poor configuration, which allows attackers to easily compromise them [6]. According to [17], hacking a typical device takes around two minutes since manufacturers tend to use publicly available and sometimes hardcoded administrative passwords. Tools such as *Shodan* and *IoTseeker* can be easily employed to discover such vulnerable devices. This brings the important question of how can large-scale exploitation of such vulnerabilities be prevented, as IoT devices have very limited capacity for securing themselves; they cannot be equipped with the operating systems or the multitude of security mechanisms available on a desktop computer. Moreover, a software update method to fix vulnerabilities and update configuration settings is often overlooked by manufacturers, vendors, and others on the supply chain. Further, even if such functionality is given, there is often no efficient way to patch those devices, and the possibility to add new vulnerabilities exists.

Many best practices have been developed in order to address these issues. As an example, the *online trust alliance* (OTA) published an IoT trust framework for the CE devices, whose recommendations have technical counterparts that have been widely recognised to be the cornerstone towards securing the IoT. Among these security solutions, the following are priority controls to implement for enhancing attack prevention [17]:

- manage efficiently the hardware devices;
- develop an inventory of authorised software;
- protect the configurations of CE devices;
- perform continuous vulnerability assessment;
- protect sensitive data and users' privacy.

Building and managing vulnerability profiles, possibly with the involvement of manufacturers [9], can be useful as it would assure consumers that security & privacy issues are addressed seriously. Realising the above is far from trivial and blockchain may prove to be ideal toward this direction.

IV. Placing Trust on the Blockchain

Current centralised security solutions are not adequate for dealing with the waves of attacks and the heterogeneity of the IoT devices. The subsequent analysis leads to the conclusion that blockchain can be used to achieve trusted decentralised coordination among IoT devices and help defending against sophisticated attacks. It is expected to define a fundamentally different approach to security, going far beyond the device's security alone, to also include [1], [9]:

- *Identity security:* blocking theft of identity, disallowing successful use of rogue public-key certificates, countering man-in-the-middle (MiTM) attacks.
- *Data security:* preventing data tampering, developing access control mechanisms and *keyless signature infrastructures* (KSI) on the blockchain.
- *Communication security:*, protecting *domain name system* (DNS) services, stopping DDoS attacks, defending critical information infrastructures.

Specifically, the *security through transparency* approach of a public blockchain has clear advantages for the IoT compared to the usual *security through obscurity* model. The blockchain will ensure the whole structure's security due to its provable cryptographic properties.

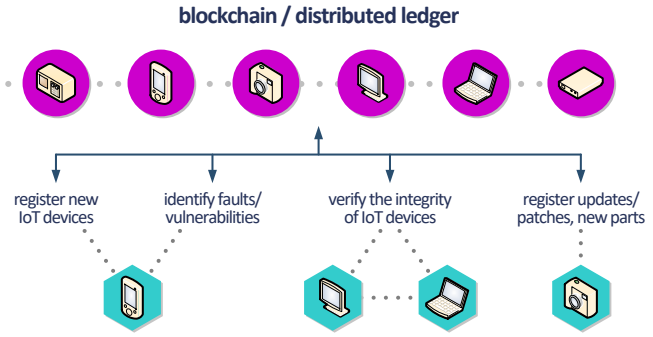

Fig. 3. The blockchain functions as a distributed transaction ledger, for various IoT transactions enhancing the security of IoT-enabled CE devices.

How will blockchain help mitigating attacks?

Attacks on connected smart devices aim at impacting their operational integrity so that they do not strictly function within their specified usage. For lightweight devices, lacking proper defence mechanisms, critical information of a manufacturer's IoT device operation could be recorded on the blockchain so that it can be later queried when e.g. a verification of proper functioning is needed, or parts of the system's software have to be updated or patched reliably (*see* Fig. 3). As also noted in [4], software updates could also be made available to the network after having been approved/validated by a majority of peers. This implies that multiple properties/aspects, such as a device's firmware, the operating system and critical software, the system/network configuration files, and audit or event logs could be verified against a history of previously valid states, to ensure their integrity. Such information could be monitored on a continual basis for illicit changes and proper actors, e.g. the IoT service provider or the device owner, could be alerted in case of verification failure. This approach fits well within the current practices of the software distributors that publish the hashes of their software binaries to allow users verify the

TABLE I
MALICIOUS ATTACKS TO BLOCKCHAIN AND DEFENSIVE MEASURES [20].

Attack	Definition	Defensive measures
Double spending	More than one payment is made with a body of funds	Complexity of mining process
Record hacking	Blocks in the ledger are modified, or fraudulent transactions are inserted	Distributed consensus
51% attack	Miner of computational power more than the rest of the network, which dominates the verification process	Detection techniques and robust incentives design
Identity theft	The private key of an entity is stolen	Identity reputation blockchains
System hacking	The software systems that implement a blockchain are compromised	Robust systems; advanced intrusion detection

TABLE II
TAXONOMY OF VULNERABILITIES IN SMART CONTRACTS [12].

Vulnerability	Cause	Level
Call to the unknown	The called function doesn't exist	Contract's source code
Out-of-gas send	Fallback of the callee is executed	
Exception disorder	Irregularity in exception handling	
Type casts	Contract execution type-check error	
Re-entrance flaw	Function re-entered prior termination	
Field disclosure	Private value published by miner	
Immutable bug	Contract altering after deployment	EVM bytecode
Ether lost	Send ether to orphan address	
Unpredictable state	Contract state change prior invoking	Blockchain mechanism
Randomness bug	Seed biased by malicious miner	
Timestamp dependence	Malicious miner changes timestamp	

authenticity of their copy [14]. Thus, to achieve an enhanced security for IoT-enabled CE devices, the following phases in their life-cycle should be considered as shown in Fig. 3.

Registration: When a product is assembled, it is registered into a blockchain, hence linking the cryptographically secure fingerprint of the product to an entry in the blockchain.

Update: Upon change, e.g. update of a product's firmware, a new fingerprint is generated and submitted to the network of peers who will simultaneously insert the fingerprint into their local copies of the blockchain via a consensus algorithm.

Verification: At any point, the peers can quickly verify the properties of an IoT device by regenerating the cryptographic fingerprint; comparison of this value against the (correct) entry in the blockchain will then be used for proving the device's integrity. The advantage of using the blockchain for integrity is that there are no keys to compromise; as a result, storing a device's update history on a distributed ledger makes this data to be trusted. The assumptions under which such mechanisms are secure are the security of the hash algorithm, as well as, the transparency of the evidence —i.e. the publicly available fingerprint stored on the blockchain.

Can devices establish mutual trust?

As already noted in [7], the information on the blockchain could be leveraged to allow devices establish trust relations, or be trusted by the network. For instance, the implementation of CE device *blacklisting* by network operators has been recently suggested as the means of protection against devices that are considered as ultimately untrusted (e.g. stolen mobile phones). The transparency of the blockchain makes it ideal for realising such practices —in a general reputation-based setting [1]— in a way that is regulated by the whole network of peer entities. Focusing on security aspects of IoT devices (i.e. information as to whether a device has been compromised or is known how to achieve this) one could consider the following to evaluate the degree to which a device can be trusted:

- Have critical files or firmware been tampered with?
- Have the latest software patches been installed?
- Is the IoT device exposed to known vulnerabilities?
- Is the network traffic generated by the device typical?

To efficiently answer these questions, the current state-of-the-art in many security areas has to be combined. Implementing controls for monitoring a device's behaviour so as to protect users' privacy is a significant open problem in the security of IoT-enabled CE devices. The *manufacturer's usage description* (MUD) specifications can be adopted for enforcing operational usage compliance and block unusual/suspicious connections or services,. Likewise, blockchain solutions, by relying on smart contracts, can facilitate the wide adoption of such practices.

How secure is the blockchain?

Research on the potential applications of the blockchain and distributed ledgers in the security area has been growing in the last few years. There have been proposals for using blockchain in the form of cryptocurrencies alternative to bitcoin (they are called *altcoins*) or as the core structure accompanied by some application-tailored consensus protocol [3]. Examples include decentralised access-control management systems, where users own and control their personal data [21], binary and certificate transparency systems [14], and cryptocurrencies to allow a device proving having contributed to a DDoS attack against a specific target [19]. The security of these proposals, wherever rigorously treated, depends on the assumptions made about the security of the underlying blockchain data structure. However, it is now well-understood that a holistic security analysis must consider cryptographic (primitives employed), software (smart contracts), and game-theoretic (incentives) aspects.

From the cryptographic viewpoint, blockchain's properties have been well-studied due to the attention gained by Bitcoin. *Persistence* and *liveness* are critical properties for blockchain security, i.e. to prevent adversaries from performing a selective DDoS attack against account holders or mining pools; it is known that these cannot hold if more than $1/2$ of the miners in a synchronous network are selfish (i.e. they do not follow the protocol) —known as the 51% attack. This threshold has been subsequently revised, using a game-theoretic approach, to letting an adversary's hashing power be less than about $1/3$ of the network's total hashing power. Since the assumption on fully synchronous networks (absence of any delays in message delivery) that is often made is unrealistic (but it gives a good sense of the security offered), recent research efforts focus on asynchronous networks to study the security of protocols being built on top of the blockchain. A synopsis of main blockchain attacks is given in Table I.

Though it is hard to modify records stored in a blockchain, it is possible to compromise the software systems implementing the technology; the hack of Mt. Gox, resulting in $450 million losses, is such a notable example. Another incident is related

to the *decentralized autonomous organization* (DAO), holding a large percentage of Ether; it suffered ∼$60 million in losses when a smart contract vulnerability was exploited leading to an infinite recursive calling situation that blocked the invocation of the function updating a user's balance; a summary of such vulnerabilities in smart contracts is provided in Table II. Many of these vulnerabilities apply to Solidity, which constitutes the high-level programming language supported by Ethereum.

V. Privacy and data protection on the blockchain

Although blockchain is being considered as a somehow *anonymous data structure*, privacy properties in this context have never been formally stated in a provable way. A common interpretation of privacy is that it should be considered as the right of an individual to control how personal information is obtained, processed, distributed, shared or used by others; i.e. it is related to the so-called personal data processing. The term *personal data* refers to information relating to an identified or identifiable natural person —a person who can be identified, directly or indirectly. However, to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used for identifying the natural person directly or indirectly. Hence, personal data having undergone pseudonymisation that could be attributed to a natural person by using additional information, should be considered to be information on an identifiable natural person.

In the case of incorporating blockchains in IoT technologies, the IoT devices will exchange information via the distributed ledger and smart contracts. In this scenario, each device can be singled out, roughly resulting in *device fingerprinting* as each device leaves a unique trace. Hence, when a device is associated with an individual, then personal data processing is in place. The above are in accordance with the new European *general data protection regulation* (GDPR) EU 2016/679 that defines the notion of personal data explicitly and states that pseudonymisation should not be considered as anonymization, though it may reduce the risks to the data subjects concerned. The GDPR is of utmost importance since it applies to organisations *regardless their location* if the subjects whose personal data are processed reside in the EU. It is thus expected that the GDPR will apply to the majority of organisations, even if they lack establishments in the EU.

Therefore, personal data protection issues in the blockchain are related to pseudonymisation and other privacy enhancing technologies that may be adopted for reducing privacy risks, like users' behaviour profiling without their consent. Clearly, the specific context of the blockchain under consideration is crucial for determining the associated risks; these are higher in permissionless ledgers, where anyone can view the whole history of transactions. Several approaches for mitigating privacy issues have been proposed, where the majority concerns cryptocurrencies like Bitcoin. However, these may also apply appropriately adjusted to blockchain for IoT security, as their goal is to avoid having user information revealed, which could leave space for privacy risks; monitoring users' activities for profiling purposes through automated decision-making tools is a typical example that poses significant risks for individuals' rights and freedoms.

The use of mixing schemes is a notable privacy enhancing approach, where many users' transactions are mixed together; however, the need for a third party raises security issues and is not desirable [13]. As a response, effort has been put to get mixing schemes operating in a transparent way so as to verify their proper operation [2]. In any case, the privacy obtained by such schemes needs to be evaluated since partial information leakage still occurs. Another approach rests with cryptographic *zero knowledge* (ZK) proofs, which are techniques allowing two parties to prove that a statement is true without revealing any information. A particular ZK proof does not necessitate the interaction between prover and verifier and is called *ZK succinct non-interactive argument of knowledge* (zkSNARK). This tool has been proposed for achieving anonymity in the blockchain —with the Zerocash system being a characteristic example [16]. Its main idea is that a transaction's creator can prove that the transaction is true without revealing sender's or receiver's address and the transaction amount. A more recent approach is the design of a privacy preserving distributed file storage system relying on the blockchain for handling funds, while storage providers have financial incentives to contribute [8]; a privacy preserving payment mechanism, based on ring signatures, and one-time addresses are at the core of system's design. Although the above approaches mainly target at the financial sector, the mathematical tools they are based on may also be applied, as stated above, to blockchain applications for the IoT industry. In any case, it is evident that privacy issues are not fully resolved and further research is needed.

Another challenge that blockchain applications may need to address, to ensure compliance with the regulatory framework in force, is how to erase personal data from the ledger if a user revokes his consent for the processing of data —referred to as the *right to be forgotten* in the GDPR. By recalling that data in a blockchain are in general personal, such a functionality seems to contradict the immutability property of blockchains. Towards this end, a number of solutions could be considered. For instance, the blockchain can contain the hash values of the transactions and not the transactions themselves, which could be stored separately; hence, deleting the separate transactions seems to address the right to be forgotten —as a direct result of the irreversibility of the hash values— without affecting the overall structure of the blockchain.

VI. Current market situation

Several industry players have already delivered blockchain-based solutions, or have joined international initiatives, aiming at strengthening the IoT. The partnership of IBM and Samsung Electronics led to the *autonomous decentralised P2P telemetry* (ADEPT) platform [1]. For building a fully decentralised IoT, a number of functionalities were established —P2P messaging, distributed file sharing and autonomous device coordination— using open source protocols. In particular, Ethereum was used for device coordination, delivering functions like registration, authentication and consensus-based blacklisting, thus allowing to establish mutual trust relations among the devices. Gladious presents an interesting approach for mitigating DDoS attacks with the use of blockchain, where the pools of nodes will be

dynamically formed (by means of Ethereum's smart contracts) in order to validate requested connections and block malicious activity; such an approach could be used to protect IoT devices having weak/no security capabilities from being compromised by accepting malicious connections. Other blockchain security tools for the IoT, like Factom, Filament, and Guardtime, have been developed (*see* [1]) focusing on safeguarding the integrity of system components or that of data records.

The vast number of applications, across many industries and sectors, that could benefit from the blockchain leads to diverse requirements that cannot be met by a particular choice of DLT model or consensus protocol. The Hyperledger project, which is hosted by the Linux foundation, is a collaborative effort, by industry leaders in finance, banking, technology, supply chain, etc., aiming at creating open-source DLT frameworks that will be the basis for building industry-specific blockchain solutions. Amongst the developed frameworks, Hyperledger Fabric has a lot of momentum, as it provides all components needed to run enterprise private blockchains. The software features that are provided are normally not available in public blockchains, like multiple confidential blockchains, near-immediate transaction finality, and no forks. Given the heterogeneity of the IoT, the Hyperledger Fabric allows making choices to meet user needs and easily deploy enterprise grade applications. Implementing a global ledger of public IoT devices requires first solving the scalability problem related to *the price of a public blockchain transaction and storage*. Using a private blockchain still has great advantage over a centralised solution: it allows common management of a shared infrastructure with no need for being maintained by a third-party. IoT actors could join and make enforceable rules regarding device management.

VII. Conclusions

IoT devices have a reputation for being critically vulnerable with a collective power allowing them to impact targets beyond a typical attacks' scope. Blockchain seems to offer the tools needed for enhancing the security of IoT devices and address key challenges. The ability to define a framework for trusted transaction processing and coordination will allow IoT devices to communicate with the increased transparency and auditing that is necessary in a world of connected things. However, as blockchain products are being developed, compliance with the data privacy legislative and regulatory framework in force need also be taken into account, as it may affect important aspects of an envisaged solution. The fact that no blocks are removed from the blockchain raises another crucial issue, which is the need to offer long-term security.

VIII. Acknowledgements

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.

IX. About the authors

Nicholas Kolokotronis (nkolok@uop.gr) is an Assistant Professor at the University of Peloponnese, Greece. He holds a Ph.D. degree (2003) in cryptography from the University of Athens, Greece. He has held visiting positions at a number of academic institutions, where he has extensively participated in security research and consulting projects. His research interests span the broad areas of cryptography and security.

Konstantinos Limniotis (klimniotis@dpa.gr) is with the Hellenic Data Protection Authority, Greece. He received the Ph.D. degree (2007) in cryptography from the University of Athens, Greece. He is currently an adjunct Faculty member at the Open University of Cyprus. His research interests include cryptography and personal data protection.

Stavros Shiaeles (stavros.shiaeles@plymouth.ac.uk) is a Lecturer in cybersecurity at Plymouth University, UK. He has extensive industry experience and holds various professional certificates in cybersecurity, like CEH, CAST611 and CCNSP. His research interests include digital forensics, intrusion prevention detection and response, social engineering, denial of service attacks, OSINT, insider threats, and malware.

Romain Griffiths (romain.griffiths@neofacto.com) graduated from EPITA computer science school, France, and holds an M.Sc. degree in information systems from Stevens Institute of Technology, NJ, USA. He is the CTO of Neofacto, France, and a technical advisor of Scorechain SA, Luxembourg, both companies specialising in Blockchain technologies.

References

[1] S. Bogart and K. Rice (Oct. 2015). Blockchain technology. Needham & Company, LLC.
[2] J. Bonneau, *et al.*, "Mixcoin: anonymity for Bitcoin with accountable mixes," in *FC 2014*. LNCS 8437, pp. 486–504, Springer, 2014.
[3] J. Bonneau, *et al.*, "SoK: research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE SP*, pp. 104–121, 2015.
[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[5] P. Corcoran, "The Internet of things: why now, and what's next?," *IEEE CE Mag.*, vol. 5, no. 1, pp. 63–68, 2016.
[6] J. Decuir, "The story of the Internet of things: issues in utility, connectivity, and security," *IEEE CE Mag.*, vol. 4, no. 4, pp. 54–61, 2015.
[7] IBM (Jun. 2017). Tomorrow's value chain: how blockchain drives visibility, trust and efficiency.
[8] H. Kopp, *et al.*, "Design of privacy-preserving decentralized file storage with financial incentives," in *2017 IEEE EuroS&PW*, pp. 14–22, 2017.
[9] N. Kshetri, "Can blockchain strengthen the Internet of things?," *IEEE IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.
[10] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry," *IEEE CE Mag.*, vol. 6, no. 3, pp. 19–23, 2017.
[11] J.-H. Lee and H. Kim, "Security and privacy challenges in the Internet of things," *IEEE CE Mag.*, vol. 6, no. 3, pp. 134–136, 2017.
[12] X. Li, *et al.*, "A survey on the security of blockchain systems," *Future Gen. Comput. Syst.*, 2017.
[13] S. Meiklejohn, *et al.*, "A fistful of bitcoins: characterizing payments among men with no names," in *2013 ACM IMC*, pp. 127–140, 2013.
[14] M. Melara, *et al.*, "CONIKS: bringing key transparency to end users," in *24th USENIX Security Symp.*, pp. 383–398, 2015.
[15] M. Peck, "Blockchains: how they work and why they'll change the world," *IEEE Spectrum*, vol. 54, no. 10, pp. 26–35, 2017.
[16] E. Sasson, *et al.*, "Zerocash: decentralized anonymous payments from bitcoin," in *2014 IEEE SP*, pp. 459–474, 2014.
[17] Symantec (Apr. 2017). Internet security threat report, vol. 22.
[18] H. Thapliyal, "Internet of things-based consumer electronics," *IEEE CE Mag.*, vol. 7, no. 1, pp. 66–67, Jan. 2018.
[19] E. Wustrow and B. VanderSloot, "DDoSCoin: cryptocurrency with a malicious proof-of-work," in *10th USENIX WOOT*, pp. 1–10, 2016.
[20] J. Xu, "Are blockchains immune to all malicious attacks?," *Financial Innov.*, vol. 2, art. 25, pp. 1–9, 2016.
[21] G. Zyskind, *et al.*, "Decentralizing privacy: using blockchain to protect personal data," in *2015 IEEE SPW*, pp. 180–184, 2015.