Blockchain-based Cyber Physical Trust Systems

Arnold Beckmann^1, Alex Milne^1, Jean-Jose Razafindrakoto^1, Pardeep Kumar^1, Michael Breach^2, Norbert Preining^3

^1 Swansea University
^2 Oyster Bay System, Swansea
^3 Accelia, Tokyo

Abstract

Cyber Physical Trust Systems (CPTS) are Cyber Physical Systems and Internet of Things enriched with trust as an explicit, measurable, testable system component. In this chapter, we propose to use blockchain technology as the trust enabling system component for CPTS. Our proposed approach shows that a blockchain based CPTS achieves the security properties of data authenticity, identity and integrity. We describe results of a testbed which implements a blockchain based CPTS for physical asset management.

Keywords: Cyber Physical Systems, Internet of Things, data authenticity, identity, integrity, asset management

1. Introduction

Cyber Physical Systems (CPS) integrate computation, networking and physical processes [1]. As CPS and Internet of Things (IoT) are quite overlapping, the distinction to IoT is blurred, with CPS serving as IoT devices, and IoT devices being components of CPS. Advances enabled by CPS are vast, including electric power generation and delivery, personalized health care, traffic flow management, and emergency response, as well as in many other areas now just being envisioned. As shown in Fig. 1, many millions of connected CSP devices will be communicating over the public network and will be providing services to their respective applications.

For many applications of CPS, the identity of devices and data generated by devices form an important part of the overall ecosystem they are integrated in. Often there are a number of actors, which may be devices or humans, that participate in such ecosystems, and who in general do not trust each other. While some actors may interact with devices directly, they often share virtual representation of device identities and their data. The challenge in such a situation is how actors can gain trust in the integrity of identities and data in an explicit, measurable, testable way. Trust can be defined as *reliance on the character, ability, strength, or truth of*

someone or something; one in which confidence is placed [2], or as *the firm belief in the reliability, truth, or ability of someone or something* [3].

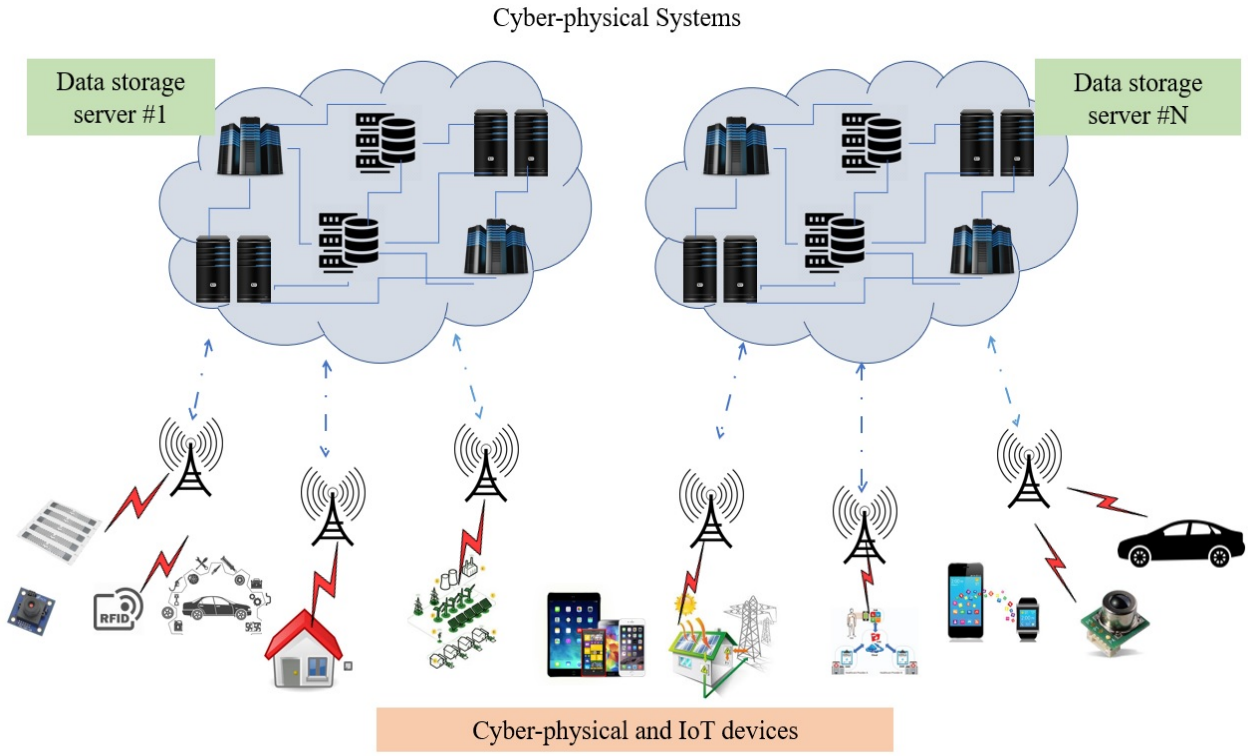

Figure 1: Connected Cyber Physical System.

We define *Cyber Physical Trust Systems* as CPS which have explicit mechanisms for gaining trust on integrity of identities and data build into them. This has to be contrasted to trustworthiness of CPS, which is the combination of security, privacy, safety, reliability, and resilience [4]. Trustworthiness is a property which is implicit to CPS, often established as a form of certificate. It cannot be tested on a CPS system level but exists externally to it.

Definition [Cyber Physical Trust Systems (CPTS)] *A* Cyber Physical Trust System *integrates computation, networking, physical processes, and explicit mechanisms for gaining trust in integrity of data about processes.*

In this chapter, we propose to use blockchain technology as a way of establishing explicit mechanisms for gaining trust. A blockchain (or ledger), as its name suggests, is a growing chain of blocks that contain transaction data of various kind — such as financial transactions related to exchange of assets — and linked together using cryptography. On a blockchain, transactions are recorded chronologically, forming an immutable chain — hence, making its data verifiable and auditable. The ledger is distributed across all participants in the network. And because of the immutability property of the blockchain, and a clever mix of cryptography and game theory, everyone in the network agrees with a single copy of the blockchain. Figure 2 shows a pictorial high-level view of a blockchain.

In addition to being a system of record, a blockchain can also be a platform for smart contracts. Basically, a smart contract is an autonomous agent stored on the blockchain and is encoded as part of a special transaction, which introduces the contract to the blockchain. One can also view a smart contract as a state machine with its current state somehow represented on the blockchain. Any transaction invoking a smart contract stored on the blockchain will trigger its execution. Once it finishes executing, all relevant actors in the network will unanimously agree on the new state of the smart contract and record that state on the blockchain.

There are different types of blockchains. The most widely used type of blockchains are of public type. In a public blockchain, such as Bitcoin [17] or Ethereum [18], anyone can participate without permission. However, one can also have permissioned blockchains. Such blockchains are built such that they grant special permissions to each participant for specific functions to be performed – such as read, write and access information on the blockchain. Here, we are mainly focused on permissioned blockchains; and in particular, the Hyperledger Sawtooth, which is an open source project originally developed by Intel [19] and now under the Hyperledger umbrella. Among the consensus options in Sawtooth, there is a novel consensus protocol known as "Proof of Elapsed Time", a lottery-design consensus protocol that optionally builds on trusted execution environments provided by Intel's Software Guard Extensions (SGX) [19].

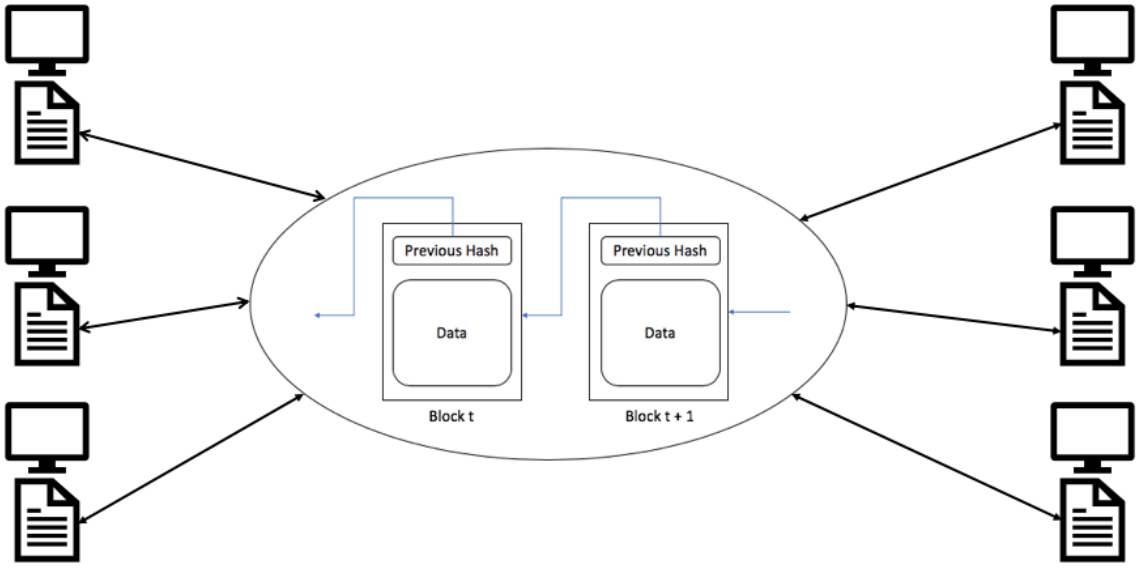

Figure 2: A pictorial representation of a blockchain.

As an application of CPTS we will consider traceable assembly systems. Assets as assembly systems are ubiquitous in our modern world. For various societal and economic challenges, it is essential to provide identities to components of assembly system, and to enable a group of

untrusted economic players to create trust about identity and usage of such components. Use cases can be found in circular economy (trust in usage of components enables reuse and supports recycling), subscription models (instead of consumer owning assets, e.g. cars, ownership is retained with manufacturer and consumer subscribe to asset pools of various quality), preventing fake parts in the automobile industry [20], and various other models of refined distributed ownership of assembly systems.

Traditional identity management are not able to provide the required level of trust in the identity and usage of assembly systems and other real-world CPS. We have taken a different approach based on blockchain, employing blockchain's data immutability and provenance, and consensus mechanisms. We obtain a blockchain based CPTS that provides trust in the integrity of identities in assembly systems and their usage data, using the following basic idea: We assume that physical components have digitally represented physical identities - there are solutions available already via security tags in the form of enhanced RFID tags which cannot be removed from physical objects without being destroyed, and which are enabled with suitable cryptographic primitives for signing data. We also assume that part of assembly systems are IoT devices for recording usage data, and that those IoT devices are enhanced by cryptographic primitives for signing data. Based on those assumptions, we have achieved a demonstrator which implements a blockchain-based CPTS for establishing trust in the integrity of identities and usage data for assembly systems. The demonstrator provides a decentralized application (DApp) consisting of a permissioned blockchain build on the Hyperledger Sawtooth framework, integrated into a wider business logic, which interacts with physical objects via simulated security tags.

The rest of the chapter is organized as follows: Section 2 discusses the state of the art work where blockchain is used as a security service. Section 3 presents an overview of use-cases and security design goals. Section 4 describes the details of the proposed technique, and Section 5 discusses the testbed results and security analysis. Finally, conclusions are drawn in Section 6.

2. Related work

Recently, blockchain as a security-service has attracted more and more attention from both academia and industry and it is spanning across several domains, including supply chain system, banking, healthcare, asset management, etc. This section presents the state-of-the-art work on the blockchain based security services (such as authentication, trust, integrity, etc.) in Internet of Things, wireless sensor networks and other domains.

In blockchain, the transaction-recording and non-duplicability services make it a good technological choice for several applications. More precisely, these services demonstrate the blockchains' suitability for public key infrastructure (PKI). Blockchain-based PKI solutions are distributed and have no centralized point of failure. As a result, certificate-based PKI can be used to realize authentication in blockchain [5][6]. However, public-key certificates have own

shortcomings and issues. In order to solve certificate issues, Lin et al. propose an identity-based linearly homomorphic signature scheme and its application in blockchain [7]. In an identity-based scheme, a node's ID can be the node's name or any arbitrary string that can be used as a public key. The encryption approach consists of four phases: setup, extract, encrypt, and decrypt. In addition, the scheme is proven to be secure against existential forgery on adaptively chosen message and identity attack under the random oracle model.

Lewison-Corella propose a blockchain based distributed database to store data securely [8]. The main idea of that paper is to allow the certificate authority (CA) to publish an unsigned certificate. The blockchain stores the hash value of the certificate and that stored value is controlled by entities, such as banks or governments. These entities make use of two blockchain databases, one for the issued certificates and another for the revoked certificates. When verifying the certificate, an entity first assures the corresponding data is stored to the blockchain. If the certificate's hash value is found in the database, then the certificate is a valid certificate. Otherwise it is not a valid certificate and then it will be revoked from the blockchain. This idea is simple and provides several advantages such as an easy verification with low delay guarantees. However, the implementation and evaluation results are missing, therefore the viability of this approach is a big question.

Lin et al. propose a blockchain based secure mutual authentication and access control system for Industry 4.0 [9]. They claim to provide various security services, including anonymous authentication, auditability, and confidentiality and privacy. The authors utilized attribute based signatures to achieve anonymous authentication and fine-grained access control. Lin et al. adopte consensus procedure, which is based on the practical byzantine fault tolerance (PBFT) approach. However, PBFT suffers from the scalability issues as discussed in [10].

As the number of Internet of Things (IoT) devices is exploding, it is almost impossible to create an efficient centralized authentication system. Hammi et al. propose a decentralized blockchain-based authentication system for IoT [11]. To achieve their goals, the proposed scheme relies on the security advantages provided by blockchains, and serves to create secure virtual zones (bubbles) where things can identify and trust each other.

Another research focuses on blockchain based digital identity management also known as "*BIDaaS: Blockchain based ID as a Service*" [12]. This research mainly targets identity management in mobile telecommunication networks. Three entities are being involved: user (e.g., mobile user), BIDaaS provider (e.g., telecommunication company), and partner of the BIDaaS provider (e.g., partner of the telecommunication company). The basic idea of the scheme is that a mutual authentication is performed between the user and the partner. The scheme did not utilize any pre-shared information or security credential shared among them. More detailed survey papers on security services using blockchain can be found in [13] and [14].

3. Overview of use-cases and security goals

Use-cases: Blockchain based approaches are popular in many real-world applications. We describe two examples which are relevant to our approach**.**

Asset management: Asset assemblies can have thousands of tracked components, e.g. for aviation assets. It is therefore crucial to have suitable asset management in place to handle the organization, identification and value creation of asset assemblies. Asset management systems also need to support the creation of subassemblies and virtual representation of them in order to reduce the underlying complexity. In the context of the need for our economies to become circular, reusing components within assets becomes a necessity. Thus, such asset management systems should also manage the accurate recording of usage against assembly systems and their components, as well as their history, in order to support value creation from reused components.

Traffic management using a smart road radar [11]: A smart road radar is a road radar that can be controlled and set up remotely without human intervention to avoid road accidents. The main responsibility of a road radar is to measure the speed of vehicles on the road. If a vehicle is violating the speed limit then the radar can detect the speed violator, and send a message including a photographed of vehicle, license plate and the measured speed to the blockchain based traffic management systems. In such a system car authenticity, identity and data integrity is of high importance.

Security goals: Following the literature survey, we have identified that a blockchain based CPTS must fulfill a number of security requirements in order to attain the sustainability and resiliency in the CPS. Therefore, this subsection describes the main security goals, as follows.

Data authentication [15]: In the real-world cyber physical system, message authentication is an important goal. Since a malicious user can easily inject fake data to a CPS, the blockchain-based systems must ensure data authenticity and check whether the data is originated from the trusted or claimed node. In general, data authentication allows a receiver entity to check the legitimacy of data that the data really was sent by the claimed entity.

Data integrity [14]: Data integrity ensures the receiver that the received data/transaction is not altered by an adversary.

Secure identity management [16]: A massive number of devices will be deployed in a CPS network, and each device will have its own identity. However, identity management can play a major role in real-world CPS network to track and trace the information/status of the devices. Therefore, secure identity management is an important requirement for blockchain-based CPTS.

4. Proposed Approach

The basic design idea of blockchain based CPTS is that CPS are linked to a blockchain ledger which is distributed amongst the actors of the ecosystem. The key blockchain features, as discussed before, will achieve that the data stored on the blockchain and smart contracts executed by the blockchain are trusted amongst the actors.

In the following we describe a scheme in which data from a CPS device will be recorded on the blockchain. For our scheme we assume that the recording is requested by one of the actors who has an interest for the data to be documented at this point in time. We assume that the actors also want to gain trust in the time when the data has been recorded, in addition to gaining trust in the data itself. The data is stored on the blockchain in an associative array, where the keys are given by the IDs of CPS devices, and the values are the process data, and the block number within the blockchain where the recording took place as a timestamp.

Our scheme has three components:

- A CPS device, that, in addition to be able to compute and to communicate, has a cryptographic identity through an asymmetric pair of keys. It is able to communicate its identity in form of its public key, to communicate data related to its processes, to receive additional data, and to sign data (i.e. its process data or received data).
- A client representing one of the actors who aims to record the current process data of the CPS device on the blockchain. All actors are registered with the blockchain. Thus, the client can interact with the blockchain by sending transactions which will be executed by the blockchain. The client can also communicate with the CPS device, and has computing capabilities, e.g. to form transactions.
- A permissioned blockchain system that stores and executes smart contracts. The actors are permissioned to interact with the blockchain, thus transaction send by them will be executed by the blockchain system.

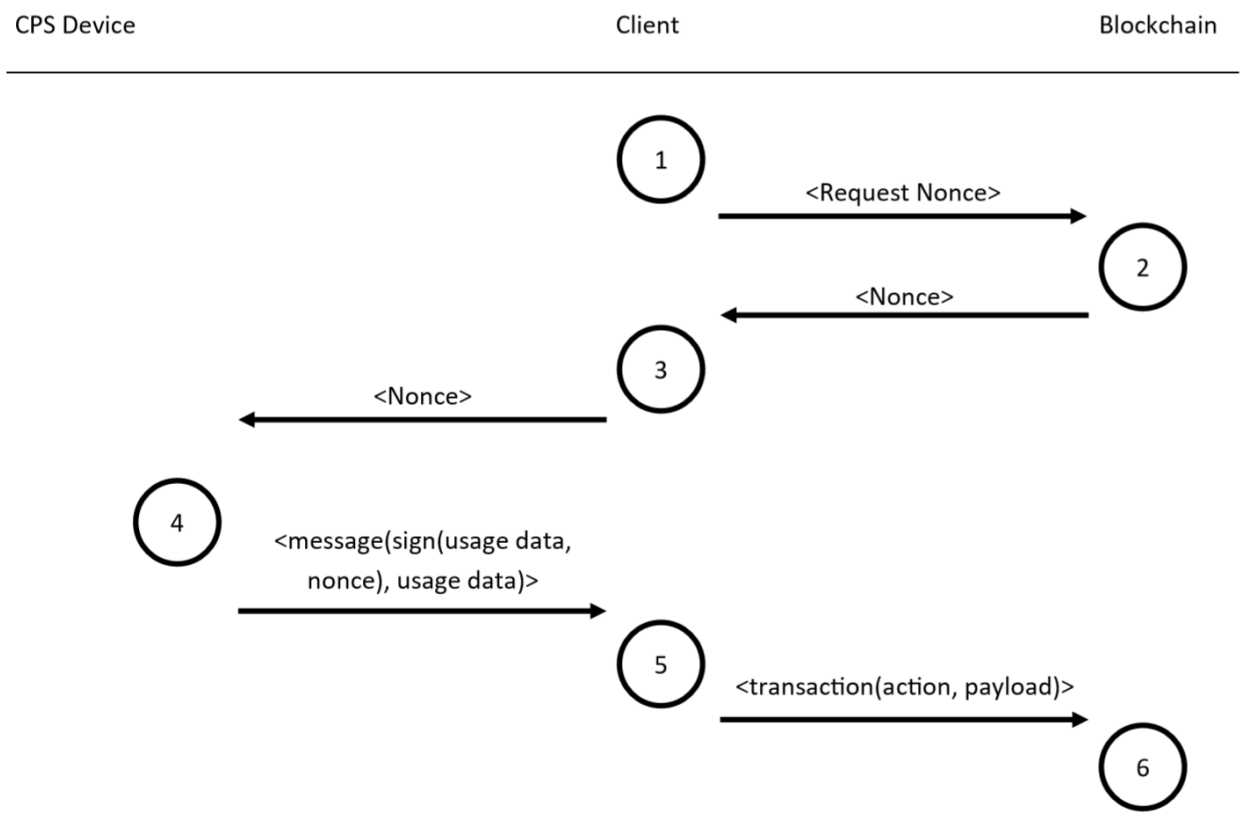

Figure 3: The proposed scheme for recording data from a CPS device on the blockchain.

The scheme then operates in the following six steps and the flow of the proposed approach is depicted in Figure 3:

1. Client wants to record process data of the CPD device on blockchain. He sends a transaction to the blockchain that requests a nonce.
2. Blockchain processes the transaction and sends nonce back to client.
3. Client requests the CPS device to sign its current process data together with the nonce.
4. CPS device sends the signed process data and nonce.
5. Client builds the transaction for the blockchain that contains the CPS device ID, signed data and nonce as its payload, the action is to record the data against the device ID on the blockchain.
6. Blockchain executes a smart contract to check authenticity of identity, data and time with the following steps:
    - Verify that the signed process data was signed by the claimed CPS device.
    - Check that the data was signed with the correct nonce and that the nonce has not timed out.
    - If all checks are true then save the data against the ID on the blockchain.

We claim that the scheme satisfies our security requirements as described above, under a set of regularity assumptions:

Claim: Assuming that the blockchain system is able to produce an unpredictable nonce, and that the cryptographic primitives are secure, data and timestamps against an ID as recorded on the blockchain are identical to the data produced by device ID at the corresponding time.

Thus this scheme achieves the security requirements of data authenticity and integrity, and secure identity management. In particular this realizes a Cyber Physical Trust System.

5. Evaluation results

This section discusses the security features and testbed results for the proposed approach.

Security features

Data authentication and data integrity: In the proposed ecosystem, each transaction of an entity uses a public key cryptography (PKC) based signature, which is generated by the private key of the entity. The inherent features of the PKC based signature *(i.e., sign(usage data, nonce), usage data)* ensures that the proposed approach can achieve data authentication and integrity.

Device Identification: Each device/entity owns an identity, which is a unique identity. Here, the identity is issued at the time of registration of devices utilizing its public key. Note that entity registration is out of scope of this chapter. However, the trustworthiness of the issued identity is assured by the signature. Each transaction of an entity is computed over its private key, and the key is only associated to the device identity. Hence, the approach can easily identify the device.

Non-repudiation: As shown in Figure 3, in each transaction, the data is signed using the private key *(i.e., sing(usage data, nonce), usage data)*, which is possesed by its owner entity. More precisely, this is the only owner who can generate and use the transaction, therefore, it cannot deny the fact of signing a message.

Secure against replay attack: A replay attack is the most common threat, where an ill-intention adversary can replay old messages. However, the proposed approach utilizes the random nonce to avoid the replay attack. Thus, an adversary cannot replay the old messages in the proposed approach.

Protection from spoofing attack: Indeed, an attacker can spoof the identity of the object from the open communication channels. However, it cannot verify the spoofed identity, as he/she does not have the knowledge of the private key of the real entity. Therefore, spoofing identity does not help him/her.

Testbed results

In the following we describe our testbed results. The testbed has been developed as part of a CHERISH-DE[1] funded Escalator project *Blockchain for Subscription Models*.

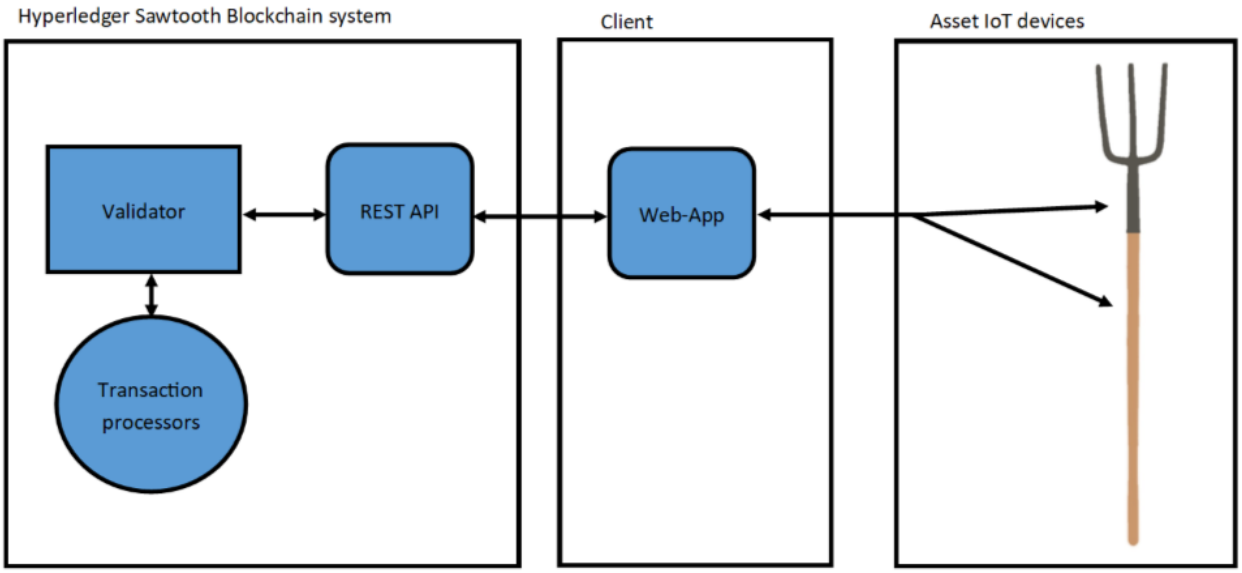

Figure 4: A simple overview of the implemented cyber physical trust system, with a gardening fork as an example asset of two components.

Testbed overview
The setup we are using is to have a blockchain system communicating through a client with a security tag/ IoT device that is attached to an asset, see Figure 4. The blockchain system we are using is Hyperledger Sawtooth v1.05. We use a client to interact with the security tag that is ingrained in the asset in order to sign data.

Hyperledger Sawtooth.
Hyperledger Sawtooth is like other blockchain systems in that its main purpose is to ensure many different parties agree on a common set of data. Sawtooth stores this data in addresses in a Merkle tree. With each change in the data the root hash of the Merkle tree changes. The current Merkle root is stored in each block as the current state of the system. Each party can verify a block by performing the given transactions from the block on their own data and then making sure that the Merkle root of the data is identical to the to the Merkle root in the block. This ensures that all parties are running code with identical effect in their transaction processors because if they were not then they would produce a different Merkle root.

IoT devices

[1] http://cherish-de.uk/ The CHERISH Digital Economy Centre is a multidisciplinary research centre at Swansea University addressing the impact of the digital economy on humans, society and industry.

In the testbed implementations, our IoT devices/ tags are attached to the asset in a way that they are not removable without destroying the device. This makes them digital representations of the physical assets. Each asset that wants to be represented on the blockchain will need to have a (digital) tag attached. These tags store a public and private key pair that are generated securely on the creation of the device and are never changeable, with the private key never been accessible outside of the chip. A tag's identity is its public key and each tag has the ability to sign data given to it to prove its identity.

Some of these IoT devices have extra functionality, the ability to track usage of the device. They store this data securely and can sign it to prove that it was in fact the usage of this asset. These tags with extra functionality will prove their identity by signing their stored usage value along with a nonce. This is of cause because allowing them to sign arbitrary data would result in an attacker being able to fake a usage not from the tag by asking the tag to sign it.

During our project we use RFID tags to emulate the functionality of these security tags. However, there are products available that realise such security tags.[2]

Client
The client is the interface that allows users to interact with the blockchain and the asset security tags. Users can query the tags to get the public key, the usage and get the tag to sign data.

The client can build transactions to send data to the blockchain to update the assets state. Some transactions are transactions to; update the usage; update the usage within a timeframe; create assets digital representation on the blockchain, assemble assets into assemblies of assets; etc.

[2] The NXP Mifare DESFire provides highly secure microcontroller-based ICs which can be used for provide security tags, see https://www.nxp.com/products/identification-and-security/mifare-ics/mifare-desfire.

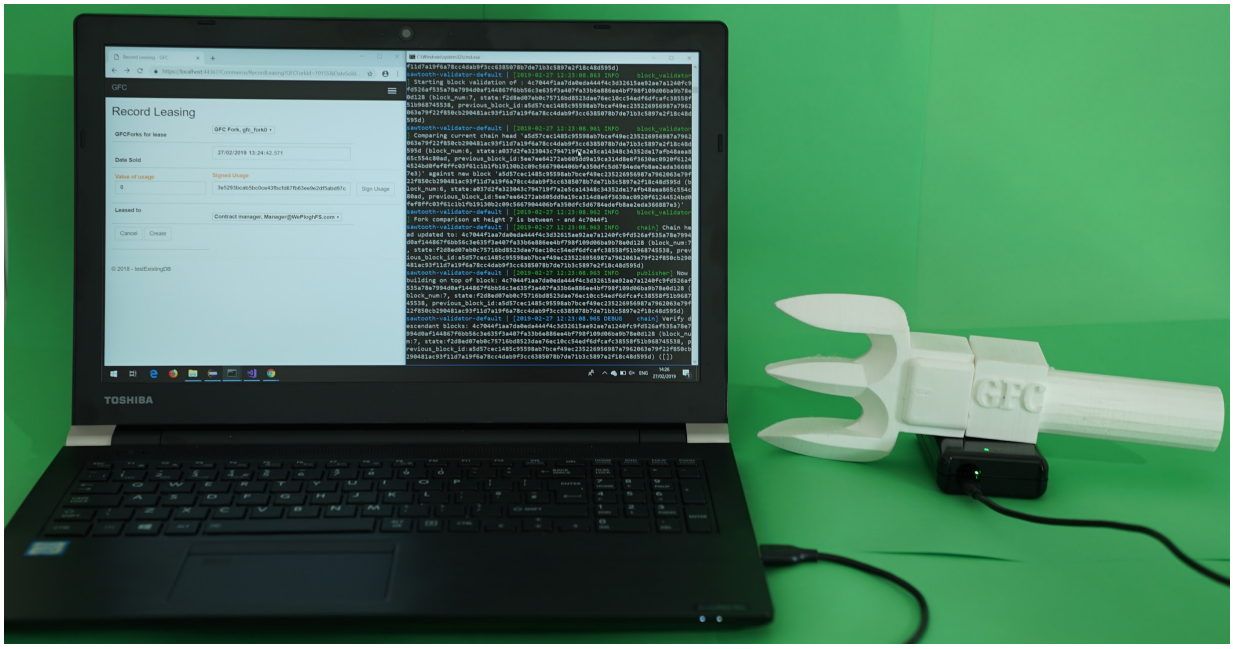

Figure 5: The running demonstrator system reading and signing, using the security tag in the fork head, the stored usage data.

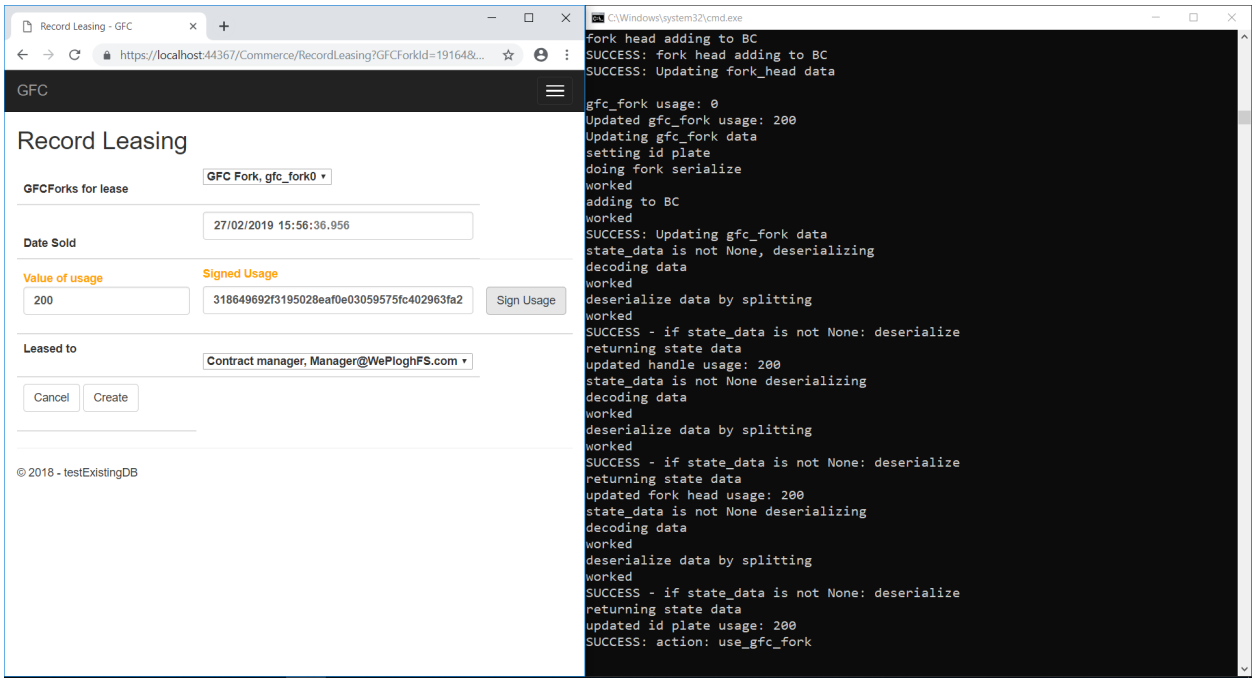

Figure 6: The demonstrator system reading and signing the security tags stored usage of 200 and then sending this in a transaction to the blockchain where it is accepted and updated.

Demonstrator

The assets in our demonstrator are forks and their security tag enhanced components. The action of starting a leasing of a fork using the web-app client can been seen in Figure 6. Here the client will get the usage and signed usage from the tag, seen in Figure 5, and send this in a transaction to the blockchain. Since the usage is used in determining the cost of the leasing in our model, it needs to be accurately updated at the start and end of a lease.

Protocol for updating the usage
The protocol for updating the usage is an instantiation of the general scheme as described before, see Figure 2. The timing requirement is implemented by using the Merkle tree root hash from the blockchain as a nonce. We can do that under the assumption that the blockchain system is in regular use (blocks are added frequently), and that not all of the transactions changing the blockchain Merkle tree can be predicted. Under those assumptions, the Merkle root hash will be unpredictable. We note that it is a general issue with blockchain systems to generate random numbers: As everyone must agree on the random number deterministically for there to be consensus, it cannot be random.

Applying our results from the previous section, we can say that the demonstrator implements a CPTS. Hence the system provides trust in the data on usage and identity of assets. Concerning time stamps it obtains a guarantee that the usage was read out from the tag within the interval between the block containing the update of the usage and the block containing the Merkle tree root that served as a nonce.

6. Conclusion

Data authenticity and integrity, and identity security are big security issues for an ever growing number of Cyber Physical Systems and IoT devices. We have introduced blockchain based Cyber Physical Trust Systems as Cyber Physical Systems enhanced with blockchain as an explicit, measurable, testable system component for providing trust in data authenticity and integrity, and identity security. We have proposed a PKC based approach for data exchange between devices and blockchain, and argued that it achieves the security requirements of data authenticity and integrity, and identity security. We presented results from a testbed that implemented a Cyber Physical Trust System for asset management.

In future work, we will conduct in depth formal and informal security analysis of our proposed scheme. We will also extend the testbed into a generic application for supporting Cyber Physical Trust Systems, and conduct in depth performance analysis ranging from theoretical ones based on theoretical performance assumptions of blockchain technology, to practical ones in relation to an enhanced testbed implementation. We will also explore other application domains, in which Cyber Physical Trust Systems can be applied.

References

[1] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems - A Cyber-Physical Systems Approach,* Second Edition, MIT Press, 2017.

[2] trust. 2019. In *Merriam-Webster.com*.
Retrieved February 24, 2019, from https://www.merriam-webster.com/dictionary/trust.

[3] trust. 2019. In *Oxford Online Dictionary*.
Retrieved February 24, 2019, from https://en.oxforddictionaries.com/definition/trust.

[4] *Framework for Cyber-Physical Systems, Release 1.0*, Cyber Physical Systems Public Working Group, National Institute of Standards and Technology, 2016.

[5] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI Around with Decentralized Automated Incentives," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 410-426.

[6] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain-based trust & authentication for decentralized sensor networks," in arXiv preprint, 2017.

[7] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen and Y. Tang, “An ID-Based Linearly Homomorphic Signature Scheme and its Application in Blockchain,” IEEE Access, Digital Object Identifier 10.1109/ACCESS.2018.2809426, 2018.

[8] K. Lewison and F Corella, “Backing Rich Credential with Blockchain PKI,” Tech. Rep. 2016.

[9] C. Lin, D. He, X. Huang, K.K R. Choo, and A. V. Vasilakos, “BSeIn: A Blockchain Based Secure Mutual Authentication With Fine-grained Access Control System for industry 4.0,” Journal of Network and Computer Applications, pp. 42-52, 116 (2018).

[10] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in International Workshop on Open Problems in Network Security, 2015, pp. 112-125.

[11] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A Decentralized Blockchain-based Authentication System for IoT,” Computer & Security, pp. 126-142, 78 (2018).

[12] J. H. Lee, “BIDaaS: Blockchain Based ID As a Service, ”IEEE Access, Digital Object Identifier 10.1109/ACCESS.2017.2782733, 2017.

[13] I.C Lin and T.C Liao, “A Survey of Blockchain Security Issues and Challenges,” International Journal on Network Security, vol. 19, no. 5., pp. 653-659, September 2017.

[14] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security Services Using Blockchains: A State of The Art Survey,” IEEE Communications Surveys, & Tutorials, DOI 10.1109/COMST.2018.2863956, 2018.

[15] M. A. Khan and K. Salah, “IoT Security: Review, Blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395-411, May 2018.

[16] D. Preuveneers, W. Joosen, and E. I. Zudor, “Identity Management for Cyber-physical production workflow and individualized manufacturing in industry 4.0,” In the Proceedings of the Symposium on Applied Computing, April 09 - 07, 2017, Pages 1452-1455.

[17] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic system. Bitcoin.org, 2009.

[18] Ethereum Foundation. Ethereum’s white paper. https://github.com/ethereum/wiki/wiki/White-Paper, 2014. Retrieved February 26, 2019.

[19] Bucci, Debbie. “Blockchain and its Emerging Role in Health IT and Health-related research”. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. Retrieved February 26, 2019.

[20] “Fake Vehicle parts are on the rise,” Accessed on February 26, 2019. https://www.gov.uk/government/news/fake-vehicle-parts-are-on-the-rise.