Securing Physical Assets on the Blockchain

Linking a novel Object Identification Concept with Distributed Ledgers

Thomas Hepp, Patrick Wortner, Alexander Schönhals, Bela Gipp
Department of Computer and Information Science
University of Konstanz
Konstanz, Germany
{firstname.lastname}@uni-konstanz.de

ABSTRACT

The use of blockchain technology to track physical assets is not new. However, the state of the art concepts are not applicable due to several limitations. One limitation is the scalability of blockchains with regard to the number of transactions that can be processed by the network. The well-established technology in tracking products is based on RFID chips that can be cloned. This paper provides insights into how objects can be protected and monitored by a varnish with a unique crack pattern, as an example of a Physical Unclonable Function. The perceptual hash of the unique pattern is used to encrypt the associated data to ensure privacy. Instead of logging each event on the blockchain individually, which is not possible due to the limited transaction throughput, OriginStamp is used to preserve data integrity on the blockchain. OriginStamp aggregates events, combines them through hashing and embeds this hash into a Bitcoin transaction. Once the Bitcoin network mines the transaction into a block and confirms it, the timestamp is considered as immutable proof of existence. With this approach, the integrity of tracking data cannot be contested.

In the future, the craquelure-based tracking approach could be extended to supply chain integration to secure the origin of products, including prevention of counterfeiting, securing the place of manufacture for trademark law or state surveillance of the agricultural economy.

CCS CONCEPTS

• **Information systems** → *Information systems applications*;

KEYWORDS

Manufacturing Supply Chain, Traceability System, Blockchain

ACM Reference Format:
Thomas Hepp, Patrick Wortner, Alexander Schönhals, Bela Gipp. 2018. Securing Physical Assets on the Blockchain: Linking a novel Object Identification Concept with Distributed Ledgers. In *CryBlock'18: 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems , June 15, 2018, Munich, Germany*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3211933.3211944

CryBlock'18, June 15, 2018, Munich, Germany
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5838-5/18/06…$15.00
https://doi.org/10.1145/3211933.3211944

1 MOTIVATION

Determining the origin of a product plays an essential role in the fight against counterfeiting, in the field of trademark law or the certification of an organic product. Consumers' awareness demands a transparent supply chain to ensure, e.g. the origin of a product or quality. By having a look at food supply chains, this requirement includes ensuring that the cold chain has been adhered to for perishable products, as well as tracing the food back to the originating farm, for example. To track products seamlessly, they must be detected by sensors and stored in a tamper-proof storage so that the user can be sure that his product is not spoiled, for example, because the cold chain has not been maintained.

A challenge for tracking products is the individual feature to be recorded. One possibility is working with active or passive RFIDs [21] or BLE [6]. The major drawback of these technologies is that they can be copied, so it would be possible to create a fake history of a product. RFID is therefore suitable as a tracking method, but not as a security feature. Hence, in the past credit card fraud was purged by adding further security features beyond the RFID technology [1]. Another big challenge is the integrity-preserving storage of the data. However, certifications like Marine Stewardship Council (MSC) as a neutral third party are able to track the path of seafood to the consumer via these technologies by providing the consumer with information, e.g. catch methods used, location caught, and species targeted. But it is not possible to trace the path of transportation. So, there is an information asymmetry between the fishing company, MSC and the consumer of the seafood. Customers must trust the manufacturer or the third party that the data hosted on a central server has not been altered or deleted. Therefore, this type of supply chain is not transparent to customers and additionally seams susceptible to manipulative interventions.

In 2008 Nakamoto [15] introduced Bitcoin, a peer-to-peer cash system based on the blockchain, which is on the one hand considered to be immutable due to cryptography and decentralization. Hence, Tracking the supply chain is more transparent by using a blockchain. Apart from these strengths, the Bitcoin network is considered slow and volatile. Due to the decentralization, the clients have to synchronize each other when a new block is mined. The blocktime is set to ten minutes, which means that about seven transactions per second can be processed [31], which is far too little for tracking products. An example of the food supply chain: if we assume that each human eats an apple a month, there is a total amount of 84 billion apples a year, which must be tracked. Tracking processes can be on leaving the plantation, transportation, storage,

[1] https://www.technologyreview.com/s/411444/rfids-security-problem/

transportation to the supermarket. So just for these apples, at least four transactions will be necessary. If we multiply this by 84 billion apples, this results in 334 billion transactions per year and 1065 transactions per second.

In the following work, we present a novel approach to secure physical products based on *craquelure* lacquers, which are considered *Physical Unclonable Functions* (PUFs) [12]. We also show how OriginStamp, a free trusted timestamping service using the Bitcoin blockchain, protects the data integrity and finally combines the physical world with the strengths of blockchain architecture. Moreover, our new approach scales in contrast to the current state of the art, because multiple events are merged into a single transaction. This work addresses the research question of *how the origin of a product can be represented transparently and immutable with the help of the blockchain.* For this purpose, state of the art is analyzed in Section 2. The strengths and weaknesses of these approaches are identified. In Section 3 our novel concept is proposed, which addresses the limitations of the state of the art. We conclude our new concept in Section 4 and identify future research directions that have been revealed by our novel approach.

2 RELATED WORK

In the following section, we examine the state of the art and explain how the real world can be transferred to the digital world by preserving the integrity of the product history. During our literature search, we identified work on supply chain integration, which is highly related to our approach. Therefore, we will investigate which blockchain-based approaches for securing physical assets already exist and identify their strengths and weaknesses.

Korpela et al. have investigated the design principles for such a system in a study [11]. Another result of their survey is the requirement for the business integration of a blockchain-based approach and a taxonomy on how blockchain can be used for supply chains. In addition, it was found that there is a gap between the readiness of integration and functionality as there are still no established industry standards for some functionalities, such as timestamping of transactions. An Agri-food blockchain was proposed by Tian [23], which uses RFID tags to track agricultural products. The aim is to ensure that the origin and requirements of the cold chain are met. The cold chain is intended to ensure that products are stored or transported under prescribed conditions so that they cannot spoil. A significant disadvantage of this approach is that there is no technical approach to how the data is organized in a blockchain and how such a system must be designed. The World Wildlife Fund (WWF) in Australia, Fiji, and New Zealand, in partnership with U.S.-based tech innovator ConsenSys, tech implementer TraSeable and tuna fishing and processing company Sea Quest Fiji Ltd., have launched a pilot project for the tuna industry in the Pacific Islands that will use blockchain infrastructure to track the journey of tuna from bait to plate. [2] Toyoda et al. [24] propose a solution for the post supply chain, which describes the history from retailer to customer. Their approach was implemented using the Ethereum Blockchain. Each time a product is scanned, the ownership of a product is transferred. using Smart Contracts so that it is possible to clearly identify who had a particular product at a certain time. A major problem with this approach is the scalability of the solution. Currently, Ethereum can process about 15 transactions per second. For instance, Amazon sells 53 items per second in Germany at peak times. The solution approach is therefore not practicable at present, as the network is not scaled for this purpose. Nakasumi's approach deals with asymmetric information exchange between supply chain participants. This exchange should be carried out transparently, privacy-preserving and in a tamper-proof manner by using blockchain technology. Through homomorphic encryption [20], this approach offers the possibility to calculate different data without publishing the data [16]. According to Nakasumi, the approach ensures that users do not have to trust any third party. Supply chain on blockchain (CoC) was introduced by Xu et al. [28], which tries to solve the scalability of a supply chain blockchain. The approach uses two different blockchains: One for the reservation of blocks, i.e. anyone who wants to write in the main chain, has to reserve a block in the reservation chain where the last blocks are only available for a certain period. Therefore, this chain is not particularly large and block hoarding is prevented. Besides, the reservation chain is protected against spamming by proof of work and mining fees. The second blockchain contains the supply chain entries and a reference to the corresponding reservation block. Without a reservation, it is not possible to write into the main chain. One disadvantage of this approach is that participants have to predict when they need a block. If this prediction is incorrect, the reservation has either expired or not yet existed, resulting in waiting time for reservation.

As a result of the analysis of the related work, several results are obtained. On the one hand, most of the presented work considers RFIDs to track products. On the other hand, there are suggestions on how to map the data in a blockchain, which is not practicable due to the scalability limitations of blockchain technology. Therefore, we introduce an alternative approach to track products in a supply chain that uses a Physical Unclonable Function, which can be used for tracking and as a security feature, and OriginStamp, which was introduced by Gipp et al. in 2015 [8].

3 LINKING PHYSICAL ASSETS WITH THE BLOCKCHAIN

RFID chips, barcodes and QR codes are not suitable for securing a physical asset in a tracking process, because they can be copied. Therefore, the counterfeiters could add the tracking feature to their fake products. The idea of tracking physical objects through PUFs is not new, but there is no concept of how this immutable property can be transferred to the digital layer. The blockchain is regarded as an unchangeable data structure due to the decentralized architecture, which is why we will examine how these technologies can be used to secure the distribution pathways of products.

3.1 Craquelure-based Tracking

Counterfeiting can be found in almost industry. Especially in the pharma industry “counterfeiting or other brand-damaging event could wipe 10 percent off a company's share price” [26]. To fight against this counterfeiting, a novel tracking feature was developed, which is based on varnish. A Krakelee (craquelure) [10] is a random pattern of microcracks (hairline cracks) developing in a layer of

[2] https://theconversation.com/how-blockchain-is-strengthening-tuna-traceability-to-combat-illegal-fishing-89965

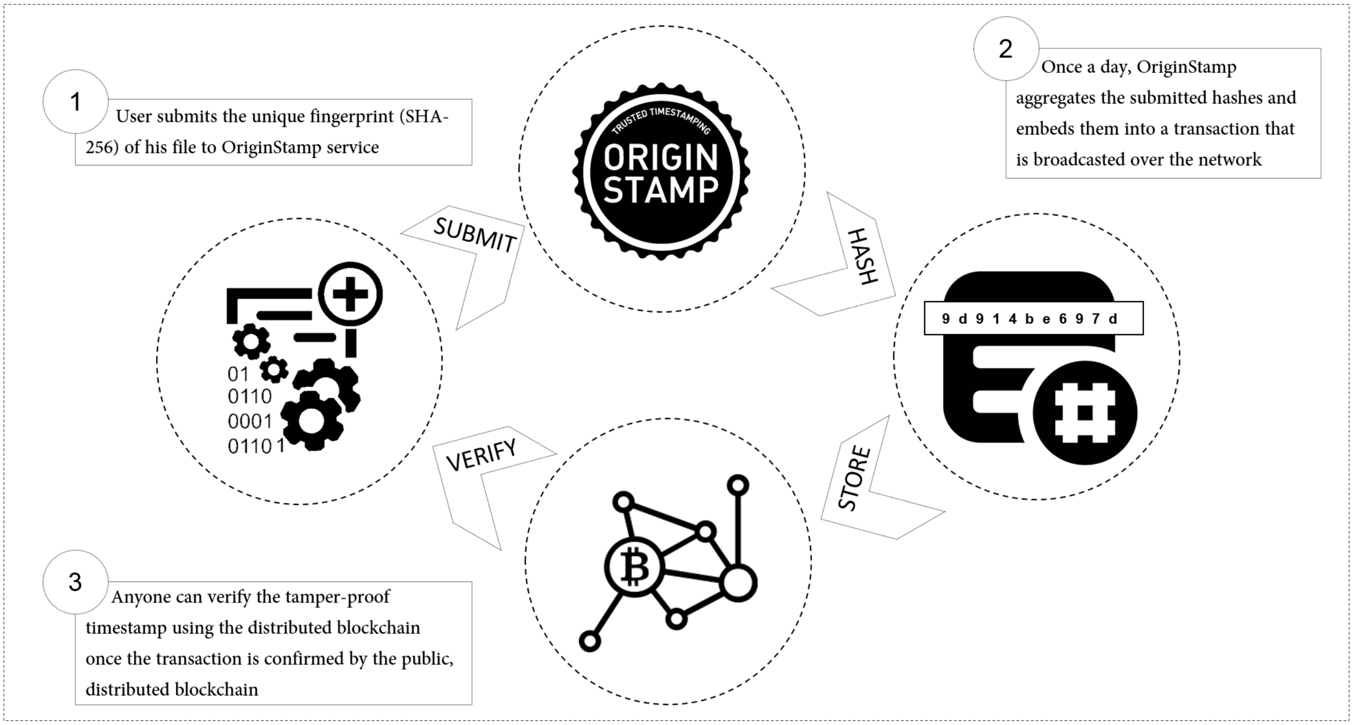

1
User submits the unique fingerprint (SHA-256) of his file to OriginStamp service
TRUSTED TIMESTAMPING
ORIGIN STAMP
2
Once a day, OriginStamp aggregates the submitted hashes and embeds them into a transaction that is broadcasted over the network
SUBMIT
HASH
9 d 9 1 4 b e 6 9 7 d
01
0110
0001
0110 1
VERIFY
STORE
3
Anyone can verify the tamper-proof timestamp using the distributed blockchain once the transaction is confirmed by the public, distributed blockchain

Figure 1: This figure from OriginStamp.org illustrates the process of trusted timestamping.

paint or varnish. The drying process results in cracks and patterns that are unique, their origin is chaotic and not predictable. The crack patterns are produced on different granularities in terms of crack size, depending on the varnish used. The resulting pattern can be read like a fingerprint for physical products. This means that each product can be uniquely identified. Some paints lead to fine cracks that can only be seen under a microscope. Other lacquers result in a rough crack pattern, which are already clearly visible on pictures taken with conventional mobile phone cameras. These are particularly suitable for use in the supply chain, as these mobile devices are accessible to the mass market. The crack pattern of the varnish is unique and if the product packaging or the product itself is provided with it, this product can also be clearly identified as shown in Figure 2.

3.2 Preserving Data Integrity with OriginStamp

Gipp et al. presented an approach to timestamp any digital content [8]. With the help of this approach, the individual stations of a product can be recorded and verified in time by storing the hash of any digital content in the bitcoin blockchain. Due to its structure, the blockchain is regarded as immutable and tamper-proof, which is why this timestamp is no longer dependent on a central instance. OriginStamp provides a *RESTful API*, which is easy and free to use for research projects. The service only needs the SHA-256 hash [9] of the digital content for timestamping. This cryptographic fingerprint does not determine the original content of the file or document, which is why the timestamp runs completely anonymously. The SHA-256-hash function is beneficial regarding this requirement since it is a cryptographic one-way function [17]. From a given hash, however, it is due to high computational complexity infeasible to determine a matching input file. OriginStamp embeds this fingerprint into the Bitcoin blockchain using a transaction. Instead of one transaction per hash, all the hashes of a period are collected, sorted alphabetically in ascending order, concatenated (*seed*) and hashed (*seed hash*) as shown in Figure 1. This so-called seed hash is then used as a private key to calculate an uncompressed Bitcoin address to which a transfer with the lowest number of Bitcoins, a so-called *dust payment*, is initiated. Unlike the RFC 3161 Standard[2], a timestamp is not dependent on a central instance and its security precautions. Even if the database is hacked or the service no longer exists in the future, the timestamps can be verified in contrast to central services, based on the timestamping process in [8]. Because many timestamps are batched into a single transaction, the cost per timestamp is also very low and any number of timestamps can be created per transaction, making scalability independent of the very limited Bitcoin blockchain. Moreover, OriginStamp does not spam the Bitcoin network with unspent outputs (UTXO), instead, the outputs are collected and the blockchain is kept clean.

3.3 Data Storage

Data in the blockchain is stored in a decentralized manner. This means data is not stored on one server as in classic software systems. Even cloud systems use centralized servers. Blockchain data is distributed over the network by connected devices, so-called nodes. Blocks are linked to each other resulting in a chained data structure. These blocks are secured by cryptography. Even in the case

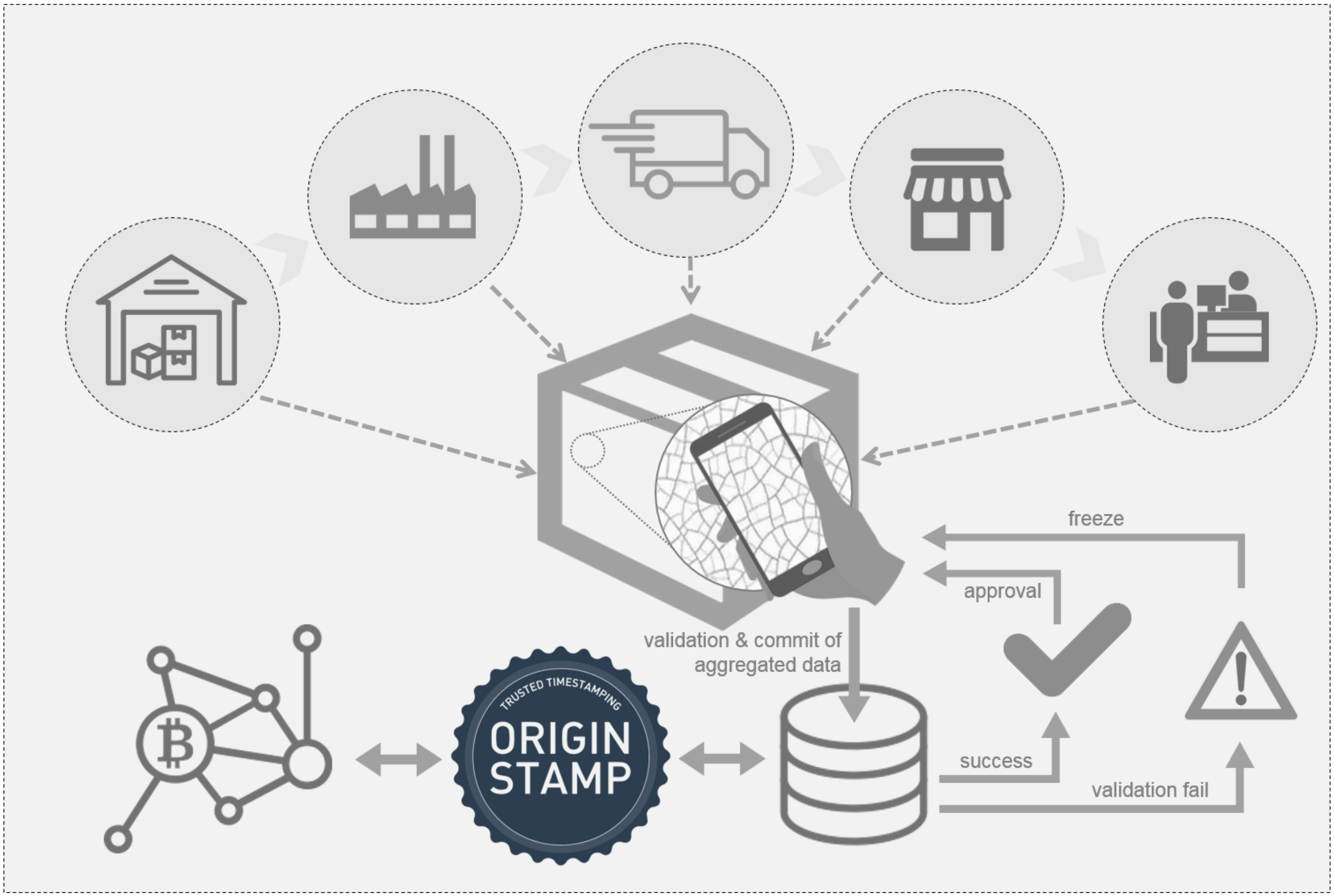


Figure 2: The figure illustrates the process of tracking a physical asset with a mobile phone camera. Each time the craquelure is scanned and verified, the corresponding meta-data, i.e. perceptual hash, location, or temperature, is encrypted, hashed, appended and finally timestamped with OriginStamp.

of manipulation, censorship or hardware failure, the blockchain will not be affected, because every node stores all information resulting in high redundancy. [22] In addition to storing data in the decentralized blockchain, data can be also managed by centralized approaches, which are introduced in the following sections.

Decentralized storage *Storing everything* in the blockchain is the simplest solution. This approach provides a high level of robustness and security due to high redundancy. But this approach has significant drawbacks: Transactions made on the blockchain are slow, e.g. the blocktime in the Bitcoin network is ten minutes. Every transaction is mined into a block, which is of limited size. So even for massive data, this approach is not recommended, because of high transaction fees and the slow transaction processing.

One example for *P2P file sharing systems* is the Inter Planetary File System (IPFS [4]. This approach is a combination of the BitTorrent protocol and Distributed Hash Tables (DHT). This flexible solution allows nodes to download selected files only. Any content is associated with a unique address and can be downloaded quickly. One drawback is that the nodes must be online, otherwise sharing and downloading is not possible. One project for better scalability is Enigma [32]; using homomorphic encryption to ensure privacy. Aspen is a service-oriented sharding approach [7]. Aspen separates disjoint transactions into asset classes, allowing users to track only the relevant chains, while protecting the entire chain with the same performance.

Cloud storage like Storj [27], Sia [25] or Ethereum Swarm are cloud file storage possibilities with hosted content on nodes. The major advantage is that not all nodes need to be online for accessing the files. This storage is highly reliable, fast, and is not limited by capacity. Moreover, the approach allows working with static files.

Distributed databases (DDB) such as BigChainDB [13] or Ties DB are other storage options. In theory, they are considered fast and provide enormous data capacity. The DDB stores all information on each block. All nodes are connected to a cluster and have full write access to the DDB. But nodes can destroy the database cluster. This DDB can also be used as a private/centralized blockchain option.

Centralized storage Almost every mentioned storage possibility can be centralized also e.g. on the server of one company. All information needs to go through a single instance. Therefore, it is easier to maintain the control over data and increase the performance in comparison to the decentralized blockchain, which requires synchronization. This approach is also much cheaper than decentralized blockchains, with transaction fees that range from several cents to over 50 dollars. On the other hand, centralized storage methods are not as trustworthy as blockchains, because the data is maintained by a central instance and not controlled by the complete network. Therefore, there is always a possibility of manipulation.

Combination of both possibilities Using DHTs, nodes can join and leave the network at any time. A DHT can set up as a network from more companies or institutions. Their data is protected by encryption and DHTs do not store all data on every node. The complexity is $O(\log n)$, where n is the number of nodes in the network. [30] Therefore, manipulation is more difficult because attackers must manipulate all nodes at once and not just a single node.

To conclude, there is no perfect storage possibility thus far. Every system or method has its own strengths and weaknesses. It is thus important to choose the right method depending on which information should be stored in the blockchain. The commonly considered criteria can include security, manipulation, scalability, type of files, or type of users. An evaluation of the different storage criteria and recommendations is provided in Xu et al. [29].

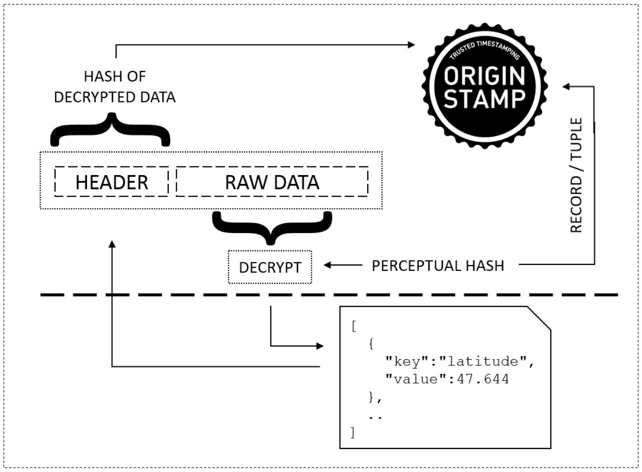
3.4 Scaling blockchain

If we take a look at supply chains for food, the exchange of information is asynchronous [15]. For the supply chain of food this can be data like certificates, videos, pictures, and other relevant documents. Scaling the blockchain is required, but not easy, because blockchain does not process transactions fast enough. Bitcoin can perform, as mentioned, only seven transactions per second. the state of the art is that every node stores all data. This leads to slow transactions rates because all nodes must be synchronized.

To solve this problem of scalability, there are different approaches, e.g. *Sharding* (partition of data to store just a part of the information in nodes) [5] or swarming (retrieving data in parallel from the nearest and fastest nodes) [19] or processing transactions off-chain like the Lightning Network [18]. Because of the massive growth of data every second, good solutions for scaling will be required.

3.5 Product Tracking Workflow

In the first step, the varnish is applied to the product or packaging. After a short drying time, the product is photographed with optical sensors. During the first scan process, the manufacturer registers the unique craquelure, which is immediately timestamped with OriginStamp. After this step, the product is verified at all subsequent stations, e.g. when it is loaded into a truck, at customs or at the retail store as shown Figure 2. The verification of our novel security feature begins with the determination of the quality of the image. The structures of the cracks can only be extracted if the image is of sufficient quality. Therefore, this quality must be determined before the actual processing with a trained model against statistical features of the image, e.g. using a Naturalness Image Quality Evaluator (NIQE) like [14]. If the quality of the input image is high enough, the lacquer cracks have to be extracted. For this purpose, neural networks are used to extract these structures. To compare existing images with each other, the image database must be searched for the most similar image. With a high number of images, many images have to be compared with each other, which can take a long time. Therefore, a perceptual hash is calculated to reduce the retrieval space and accelerate this nearest neighbor search, thus ensuring the scalability of the supply chain. If no image is found, the product has not been registered, so it could be a forgery or could be manipulated. The perceptual hash is also timestamped using OriginStamp to make scanned image verifiable at a particular checkpoint. During the evaluation of the image, meta information such as location, temperature, noise or acceleration are captured by the sensors of our mobile device.



```
[
  {
    "key":"latitude",
    "value":47.644
  },
  ..
]
```

Figure 3: The encrypted data-structure in HEX format that is stored on the server and timestamped with OriginStamp consists of mainly two parts: Header and Raw Data.

Perceptual Hash: After receiving the perceptual hash from the server, the key is converted to a public key. The data of this public key is fetched from the server and decrypted with perceptual hash. A timeline of the previous stages is visualized on the mobile device.

Sensor Data: During the evaluation of the image meta information such as location, temperature, noise or acceleration are captured by the sensors of our mobile device. The data format is converted into a JSON representation with a key-value mapping. In the next step, the data is converted into its HEX representation. In addition to meta information, a raw data set contains the hash of the last data set. This is to ensure the linkage of events.

Encrypt: The HEX data is encrypted by the perceptual hash, which is used as the passphrase. In addition, the SHA-256 of the sensor data is calculated.

Store: The raw data is generated by appending the encrypted data to the SHA-256 hash of the raw data as illustrated in Figure 3. The server validates the raw data format according to the following criteria: The first step is to check whether the transferred data is in HEX format. The header is then extracted from raw data and validated to see if it is a valid SHA-256 hash and if a timestamp already exists for it. If a timestamp already exists, the data is invalid: Because of the Perceptual Hash with identical meta information already existed before. If not, the SHA-256 [9] is timestamped with OriginStamp as explained in Section 3.2 and stored. The user can now request all data records from the operator and validate them on the client side. If a data record is missing and manipulated, the data integrity, which can be checked by OriginStamp, is no longer guaranteed. Besides, the decrypted data can be validated, e.g., the product comes from a location? Has the cold chain been maintained? In such a case, the customer may decide not to accept the product. Then a history of the product is created, which is encrypted on the server. This history is extended and displayed during each scan process. Therefore, only participants who have read the product can access the data, as they have the passphrase for decryption. On the other hand, the manufacturer can retrace the supply chain without revealing his business secrets.

4 CONCLUSION AND FUTURE WORK

In this paper, we presented a concept for linking the physical world with the digital world. This link increases transparency in supply chains, e.g. of food or medical products, through the integration of blockchain technology. The Krakelee can be used as a tracking feature, as well as a security feature, because the crack pattern is unique for each product. The effort to forge this feature is great, as the cracks would have to be imitated at nano level, which is expensive. Data integrity is ensured by OriginStamp, and the data structure only allows to append data. Therefore, a valid history of a product can be verified. However, products have to be scanned actively and do not report automatically, as for example with active RFIDs. Our new approach is the starting point for future research. Since the scalability of current public blockchains is limited, many off-chain protocols are being developed to meet the high demand. That's why our step-by-step solution uses OriginStamp, a free service for Trusted Timestamping. This ensures the data integrity of the encrypted supply chain data. Despite the higher throughputs, a private chain is not a suitable solution, since this network would be in the hands of a few companies, which could tamper with the data according to Zheng et al. [31]. The introduction of the Lightning Network [18] for the Bitcoin network has already shown how many payments can be made securely off-chain. We consider the use of a off-chain protocol, which uses hashed time-locked contracts, as a future direction of our research for increasing security and transparency for tracking physical assets. Although not every event is logged on the blockchain, the individual stages in the supply chain can be verified by OriginStamp.

REFERENCES

[1] Saveen A. Abeyratne . 2016. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *International Journal of Research in Engineering and Technology* 05, 09 (2016), 1–10. https://doi.org/10.15623/ijret.2016.0509001

[2] C Adams. 2001. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). (2001), 1–26.

[3] Andreas M Antonopoulos. 2017. *Mastering Bitcoin - Programming the Open Blockchain.* OReilly Media (2017).

[4] Juan Benet and Juan@benet Ai. [n. d.]. IPFS -Content Addressed, Versioned, P2P File System (DRAFT 3). Draft 3 ([n. d.]).

[5] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin GÃijn Sirer, Dawn Song, and Roger Wattenhofer. 2016. On scaling decentralized blockchains (A position paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9604 LNCS (2016), 106–125. https://doi.org/10.1007/978-3-662-53357-4{_}8

[6] Ramsey Faragher and Robert Harle. 2015. Location fingerprinting with bluetooth low energy beacons. *IEEE Journal on Selected Areas in Communications* 33, 11 (2015), 2418–2428. https://doi.org/10.1109/JSAC.2015.2430281

[7] Adem Efe Gencer, Robbert van Renesse, and Emin GÃijn Sirer. 2016. Service-Oriented Sharding with Aspen. (2016).

[8] Bela Gipp, Norman Meuschke, and AndrÃľ Gernandt. 2015. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. (2015), 1–6. http://arxiv.org/abs/1502.04015

[9] IETF. 2011. RFC 6234 - US Secure Hash Algorithms b(SHA and SHA-based HMAC and HKDF). (2011). https://tools.ietf.org/html/rfc6234

[10] Friedrich Kisters. 2017. Security element for marking or identifying objects and living beings. (2017).

[11] Kari Korpela, Jukka Hallikas, and Tomi Dahlberg. 2017. Digital Supply Chain Transformation toward Blockchain Integration. (2017), 4182–4191. https://doi.org/10.24251/HICSS.2017.506

[12] Roel Maes. 2013. *Physically Unclonable Functions: Construction, Properties and Applications.* Number August.

[13] Trent Mcconaghy, Rodolphe Marques, Andreas Müller, Dimitri De Jonghe, Troy Mcconaghy, Greg Mcmullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. 2016. BigchainDB: A Scalable Blockchain Database (DRAFT). *BigchainDB* (2016), 1–65.

[14] Anish Mittal, Rajiv Soundararajan, and Alan C Bovik. 2013. Making a &quot; Completely Blind &quot; Image Quality Analyzer. *Ieee Signal Processing Letters* 20, 3 (2013), 209–212. https://doi.org/10.1109/LSP.2012.2227726

[15] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org* (2008), 9. https://doi.org/10.1007/s10838-008-9062-0

[16] Mitsuaki Nakasumi. 2017. Information sharing for supply chain management based on block chain technology. *Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017* 1 (2017), 140–149. https://doi.org/10.1109/CBI.2017.56

[17] M. Naor and M. Yung. 1989. Universal one-way hash functions and their cryptographic applications. *Proceedings of the twenty-first annual ACM symposium on Theory of computing - STOC '89* (1989), 33–43. https://doi.org/10.1145/73007.73011

[18] Joseph Poon and Thaddeus Dryja. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Technical Report (draft)* (2016), 59. https://lightning.network/lightning-network-paper.pdf

[19] Narayan Prusty. 2017. *Building Blockchain Projects.* Packt Publishing Ltd.

[20] R L Rivest, L Adleman, and M L Dertouzos. 1978. On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation* (1978), 169–180. https://doi.org/10.1.1.480.3392

[21] Thorsten Staake, FrÃľdÃľric Thiesse, and Elgar Fleisch. 2005. Extending the EPC Network âĂŞ The Potential of RFID in Anti-Counterfeiting. *2005 ACM Symposium on Applied Computing* April 2016 (2005), 1607–1612. https://doi.org/10.1145/1066677.1067041

[22] Don Tapscott and Alex Tapscott. 2016. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin.

[23] Feng Tian. 2016. An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. *2016 13th International Conference on Service Systems and Service Management (ICSSSM)* (2016), 1–6. https://doi.org/10.1109/ICSSSM.2016.7538424

[24] Kentaroh Toyoda, P. Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki. 2017. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain. *IEEE Access* XXX, XXX (2017), 1–13. https://doi.org/10.1109/ACCESS.2017.2720760

[25] David Vorick and Luke Champine. 2014. Sia : Simple Decentralized Storage. (2014).

[26] Rob Whewell. 2016. *Supply chain in the pharmaceutical industry: strategic influences and supply chain responses.* CRC Press.

[27] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. 2014. Storj a peer-to-peer cloud storage network. (2014).

[28] Lei Xu, Lin Chen, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. CoC: Secure Supply Chain Management System Based on Public Ledger. *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (2017), 1–6. https://doi.org/10.1109/ICCCN.2017.8038514

[29] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017* (2017), 243–252. https://doi.org/10.1109/ICSA.2017.33

[30] Hao Zhang, Yonggang Wen, Haiyong Xie, and Nenghai Yu. 2013. *Distributed hash table: Theory, platforms and applications.* Springer.

[31] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. 2016. Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang. *International Journal of Web and Grid Services* (2016), 1–24. https://doi.org/10125/41338

[32] Guy Zyskind, Oz Nathan, and Alex Pentland. 2015. Enigma: Decentralized Computation Platform with Guaranteed Privacy. (2015), 1–14. http://arxiv.org/abs/1506.03471