script*ed*

Volume 19, Issue 1, February 2022

Blockchain-based electronic time stamps and the eIDAS regulation: The best of both worlds

Christoph Sorge and Maximilian Leicht***

DOI: 10.2966/scrip.190122.61

Abstract

Blockchain technology, introduced in the Bitcoin blockchain in 2009, can be used to ensure the integrity of data using a distributed consensus algorithm, executed by a potentially large number of participants. A variety of blockchain applications have been proposed in recent years. The distributed nature of blockchains is advantageous in many respects, but can be challenging from a legal and regulatory perspective. The European eIDAS regulation, for example, regulates trust services—but it assumes these services to be provided by individual trusted entities instead of multiple collaborating parties. We show how a particular eIDAS service, (qualified) electronic time stamps, can be seen as competing with blockchain technology. Both concepts can be used to provide proof of the existence of specific data at a certain point in time. On this basis, we explain to which extent a combination of both concepts is possible and useful in practice. This is founded on both technical and legal arguments. If the combination gains practical relevance, it may endanger a business model of trust service providers, possibly necessitating action by the state.

Keywords

eIDAS, blockchain, digital signature, electronic time stamps, qualified electronic time stamps

* Professor, Chair of Legal Informatics, Saarland University, Saarbrücken, Germany, christoph.sorge@uni-saarland.de.

** Research assistant, Chair of Legal Informatics, Saarland University, Saarbrücken, maximilian.leicht@uni-saarland.de.

1 Introduction

Since the introduction of Bitcoin[1] in 2009, the underlying blockchain technology has attracted considerable attention both in academia and practice. Using blockchain, several parties can agree on the state of a distributed database (distributed consensus) and ensure that all stored information – essentially the entire history of the blockchain – remains unchanged.[2] Numerous applications have been proposed on this basis. This includes cryptocurrencies like Bitcoin, Ether[3] or Zcash, in which the main purpose of the distributed database is to prevent double-spending, and which have been increasingly successful in recent years.[4] Blockchains (such as Ethereum) are also used as a platform for smart contracts.[5] Numerous other blockchain applications have been suggested in literature.[6]

One of the design goals of blockchain technology is to replace trust in centralized third parties by a distributed mechanism, which allows a "vote" on the correct blockchain state (e.g., based on the amount of computational power

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), available at http://bitcoin.org/bitcoin.pdf (accessed 22 July 2021).

[2] For an introduction to blockchain technology, see Zibin Zheng et. al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" (2017) *IEEE International Congress on Big Data (BigData Congress)* 557-564.

[3] The Ethereum platform's cryptocurrency, see Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger" (EIP-150 Revision), available at http://gavwood.com/paper.pdf (accessed 22 July 2021).

[4] For an overview on cryptocurrencies, see Christie Smith and Aaron Kumar, "Crypto-Currencies—An Introduction to not-so-funny Moneys" (2008) 32 *Journal of Economic Surveys* 1531-1559.

[5] For an introduction to smart contracts, see Mark Giancaspro, "Is a 'smart contract' really a smart idea? Insights from a legal perspective" (2017) 33 *Computer Law & Security Review* 825-835.

[6] For an overview, see Olga Labazova, Tobias Dehling, and Ali Sunyaev, "From Hype to Reality: A Taxonomy of Blockchain Applications" (2019) *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019)*, 4555-4564.

invested by the participants). The EU's eIDAS regulation[7], on the other hand, regulates trust services provided by individual companies, i.e., centralized third parties.

One service in particular, (qualified) electronic time stamps, which are regulated in Section 6 of the regulation, can be seen as competing with blockchain technology. Time stamps bind "data in electronic form to a particular time establishing evidence that the latter data existed at that time" (Art. 3 no. 33 eIDAS regulation). The concept has received little attention in literature but may turn out to be a valuable tool for many practical applications. For example, consider the case of renting a car. If damage is discovered upon return of the car, the question arises whether this was pre-existing damage, or whether it was caused by the current renter. The renter may even have noticed the damage when picking up the car but considered it too unimportant to bother the rental company's staff. Lengthy legal proceedings will likely follow. This situation could easily be avoided. With the use of a smartphone, photographs or a video showing all sides of the car could be recorded within a minute or two when picking up the car. A secure electronic time stamp for these photos or videos would constitute strong evidence that they were taken before the car left the premises of the car rental company and provide peace of mind for the renter. Obtaining a time stamp can be a matter of seconds if an appropriate software implementation is used. There are, of course, multiple other use cases, e.g., concerning potential intellectual property disputes.

Blockchain technology provides a technical means to achieve at least similar functionality to electronic time stamps. Blockchains can be used to ensure

[7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

immutability of data and the order in which they have been stored. We surmise that this allows, to some extent, an interchangeable use of both concepts.

In the article at hand, we introduce the eIDAS regulation (section 2) and to some technical core concepts required in the remainder of the article (section 3). Furthermore, we address the regulation of electronic time stamps in the eIDAS regulation (section 4) and some core aspects of blockchain technology (section 5). On this basis, we argue that the use of eIDAS compliant services, particularly qualified electronic time stamps, provide improved legal certainty in comparison to blockchain's purely distributed solution. In our opinion, both options are not mutually exclusive. We show, from a technical perspective, how to combine both worlds (section 6). In the next step, we discuss whether the resulting time stamps can still be considered as qualified electronic time stamps from a legal perspective (section 7), and present solution approaches to the issue of long-term security of time stamps (section 8). The adoption of the proposed combination, however, could result in remarkable economic consequences for trust service providers, potentially threatening the business model of time stamp provision. Considering the importance of time stamps, this could lead to the necessity of comparable, state-sponsored services. We discuss these aspects in section 9. Section 10 contains a discussion of a relevant proposal for amending the eIDAS regulation. We conclude the paper in section 11.

2 eIDAS regulation

In this section, we outline some basic aspects of the eIDAS regulation. The goal of the regulation is to enhance trust in electronic transactions. Therefore, it provides a common foundation of secure electronic interaction that is supposed to increase the effectiveness of public and private online services, electronic business, and electronic commerce in the European Union (EU).[8] As a regulation it is binding in its entirety and directly applicable in all Member States.[9] Nonetheless national laws may still be applicable if they do not contradict the eIDAS regulation.

In general, the eIDAS regulation aims at being technologically neutral, meaning it grants legal effects if specific requirements are met without regulating in detail how compliance with these requirements must be achieved. This is specified in recital 26 and 27 regarding the regulation itself, as well as recital 62 regarding qualified electronic time stamps.[10] However, in order to ensure interoperability and more standardized conditions the European Commission may—or in some cases was legally obliged to—adopt so-called implementing acts, which shall ensure the high level of security of electronic identification and trust services.[11] Consequently, implementing acts typically contain more concrete technical specifications, compensating the impact of the technology-neutral principle.

3 Preliminaries

In this section, we introduce some core concepts required in the remainder of the article at hand.

Digital signatures are an essential building block for internet security. They are based on asymmetric cryptography: each user has a key pair, consisting of a

[8] See recital 2 eIDAS regulation.

[9] See Art. 288 of the Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326/47.

[10] Scaramuzzino, in: Allessio Zaccaria, Martin Schmidt-Kessel, Reiner Schulze, Alberto Maria Gambino (eds), *EU eIDAS Regulation* (1st ed., Beck/Nomos/Hart, 2020), Art. 42, para. 2.

[11] See recital 71, 72 eIDAS regulation. For implementing acts based on the eIDAS regulation see e.g. Art. 23 (3), 27 (4), 32 (3) or Art. 42 (2) eIDAS regulation. For implementing acts in general see Art. 290, 291 TFEU.

private key and a public key. The private key is kept secret, while the public key is made available to communication partners. A digital signature is computed using some digital content (the *message* or *document*) and the private key. It is verified using the corresponding public key. The digital signature scheme makes sure that verification only succeeds if the following criteria are met:

- The public key used for verification corresponds to the private key with which the signature has been generated, and
- The document is identical to the one which has been digitally signed, i.e., even the change of a single bit invalidates the signature.

This implies that the private key cannot be computed from the public key. The guarantees are provided under certain computational assumptions: computation of the private key is not impossible from an information theoretic perspective, but its execution requires solving a mathematical problem assumed to be hard (computationally infeasible).[12] Informally speaking, even when using all the computational power available worldwide, the probability of an attacker finding the private key (or successfully forging a signature without the private key) within a useful time frame should be negligible. Generous security margins are usually used for the parameter choices, so that an attacker is not expected to succeed even after millions of years of computation time—unless a weakness of the digital signature scheme can be found.

The practical application of digital signature schemes requires additional concepts. Note, a public key must be securely mapped to an identity. To this end, a trusted third party (called "certification authority" in technical publications, and "trust service provider" in the eIDAS regulation) issues a certificate. In the

[12] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography* (2nd ed., Boca Raton: Chapmann & Hall, 2014), pp. 439-443.

context of digital signatures, the term refers to a signed statement confirming that a public key belongs to a certain identity. The legal term *electronic signature* is related to the technical (cryptographic) term *digital signatures*. However, in the eIDAS terminology, digital signature schemes are only required for *advanced electronic signatures* (which includes *qualified electronic signatures*).

So-called *cryptographic hash functions* are the core building block of blockchain technology. In computer science, a hash function is a function that maps an input of arbitrary length (which could be a password or an entire movie) to an output of fixed length and can be computed efficiently. A cryptographic hash function must fulfil three additional properties[13]:

(1) Given one output h(x) of the function, finding a corresponding input x should not be computationally feasible. This property is referred to as "resistance to preimage attacks". The term "computational feasibility" is used because a theoretical attacker with sufficient computational power would be able to find a preimage, given the finite length of h(x). This requirement is similar to the one stated above concerning the computation of a private key given the corresponding public key.

(2) Given one input x_1 to the function, it should not be computationally feasible to find a second input x_2 that has the same output, i.e., for which $h(x_1) = h(x_2)$. Note that there is an infinite number of input pairs which lead to the same output, as the inputs can be of arbitrary length. The requirement means that there should be no efficient way to *find* a second

[13] See William Stallings, *Cryptography and Network Security* (7th ed., Boston: Pearson India 2017), p. 349. Stallings lists the additional property of pseudorandomness, but states that it "has not traditionally been listed as a requirement of cryptographic hash functions but is more or less implied".

input with the same output. The property is called "resistance to second preimage attacks".

(3) It should not be computationally feasible to find an arbitrary pair of inputs x_1, x_2 with the same output, i.e., for which $h(x_1) = h(x_2)$. This requirement, which is called "collision resistance" is stronger than the second one. Both are still usually considered separately in literature, as they correspond to different use cases of cryptographic hash functions.

The output of a cryptographic hash function is sometimes referred to as a "fingerprint" and can be used to uniquely identify an electronic document. Cryptographic hash functions are used as a building block for practical implementations of digital signatures, which demonstrates the need for the above-mentioned properties.[14] For example, a digital signature would be worthless if an attacker could generate a second document for which the same signature is valid.

4 Electronic time stamps

The eIDAS regulation (Art. 3 no. 33) does not specify any *security* requirements for electronic time stamps in general. This means there is no unique technical procedure that is explicitly required by law.[15] Despite this lack of mandatory technical security, an electronic time stamp:

> Shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp

[14] Katz and Lindell (*supra* n. 12), p. 443f.

[15] However, see Fig. 2 and section 7 for the usual technical procedure for generating (secure) time stamps.

(According to Art. 41 (1) eIDAS regulation). We refer to the latter (i.e., electronic time stamps not meeting the requirements of qualified electronic time stamps) as *simple* electronic time stamps. In our car rental example, if information about the date and time is included as metadata within the photo or video file, this information already constitutes a simple electronic time stamp.

A *qualified* electronic time stamp must meet three additional requirements, as laid down in Art. 42: The binding between date and time on one hand and the data on the other hand needs to be secure, i.e., an undetected change of the data has to be reasonably precluded. The time stamp must be based on "an accurate time source linked to Coordinated Universal Time". Finally, it is signed by a qualified trust service provider using an advanced electronic seal, an advanced electronic signature, or an "equivalent method".

From a technical perspective, these requirements can be easily achieved if the trust service provider has access to a sufficiently precise clock. The current time, which should be specified unambiguously, is appended to the data (or a cryptographic hash value thereof). A simple, unambiguous specification of the time could include the current date, with the Coordinated Universal Time appended to avoid ambiguities due to unspecified time zones or daylight-savings time.

The trust service provider then digitally signs the result, fulfilling the requirements of an advanced electronic signature. This signature is sufficient to achieve the secure binding between time and date, and the data to be time stamped.

Fulfilling these three technical requirements leads to the legal result of the time stamp being considered 'qualified'. Therefore, it enjoys the presumption that the date and time it indicates are accurate. Also, the integrity of the data to which the date and time are bound is presumed, see Art. 41 (2). Additionally, qualified time stamps are recognized in all Member States of the EU (see

Art. 41 (3)). From a legal perspective, qualified time stamps can consequently provide more practical use-cases. They can be used whenever the existence of data at a certain time needs to be proven.[16]

5 Blockchain technology

In essence, a blockchain is a chain of data blocks, of which the following properties are usually expected:

(1) Each block contains a cryptographic hash value of its predecessor (i.e., the previous block in the chain). This guarantees that a change to one block can be detected unless all following blocks are changed accordingly.

(2) There is a distributed storage, as well as a protocol for synchronization between different nodes participating in the blockchain (usually based on a Peer-to-Peer network).

(3) There is a consensus mechanism to allow different nodes participating in the blockchain to agree on one "correct" version. In Bitcoin, this mechanism is based on the "proof of work" principle. Essentially, a version of the blockchain is considered as correct if the majority of the network's computing power has been invested in that version.[17]

In principle, arbitrary data (including photos, videos, or at least hash values of such content) can be added to a blockchain. The idea of the Bitcoin blockchain is to store transactions, while other blockchains are tailored to smart contracts. As

[16] For more use-cases see ENISA, "Security guidelines on the appropriate use of qualified electronic time stamps" (Version 2.0, December 2016), available at https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-time-stamps (accessed 22 July 2021), pp. 19-24.

[17] For introductory literature see e.g. Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps* (1st ed., Berkeley: Apress 2017); Rui Zhang, Rui Xue, and Ling Liu, "Security and privacy on blockchain" (2019) 52 (3) *ACM Computing Surveys (CSUR)* 1-34.

one block usually contains more than one data record, some data structure must be found to organize the individual records (e.g., transactions). So-called Merkle Trees (or Hash Trees, cmp. Fig. 1) are commonly used for that purpose. Instead of computing a hash value that just covers all data in the block directly, an individual hash of each record is computed first.[18] These hash values form the lowest layer (the "leaf nodes") of the tree. Several (two in the case of a binary hash tree) of these values are then concatenated, and a new hash value is computed that covers the respective leaf nodes.[19] The resulting hash values form the second-lowest layer of the tree. The process is continued until only one resulting hash value remains, which forms the root node of the tree.[20] As an advantage over other data structures, a Merkle tree allows verification of any individual records using only a part of the tree, and a smaller number of hash computations (logarithmic in the number of contained records). If properly implemented, a Merkle hash tree provides the same security as the hash function that is used in its construction.[21]

[18] See for example H(x1) in Fig. 1.

[19] See for example H(x1, x2) in Fig. 1.

[20] See h(x1...8) in Fig. 1.

[21] See Katz and Lindell (*supra* n. 12) pp. 156, 184.

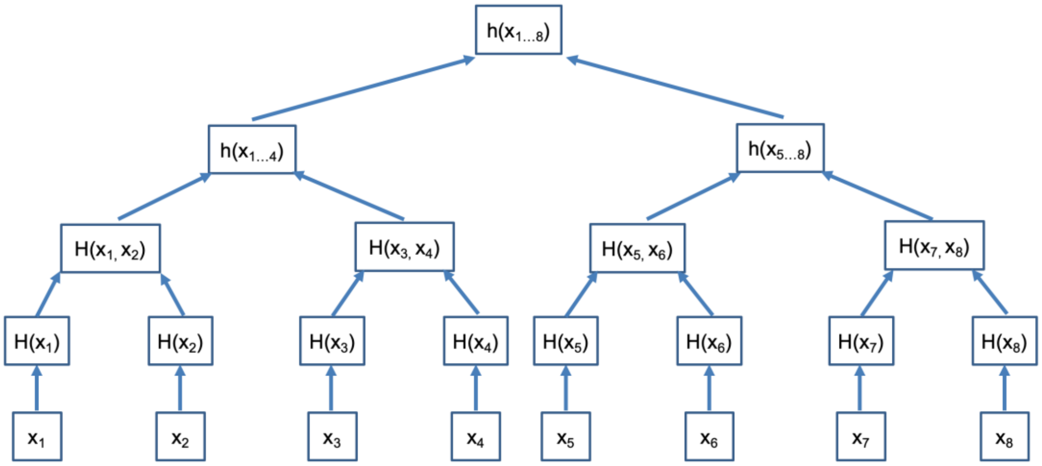

Figure 1: A Merkle tree. Figure based on Katz and Lindell (*supra* n. 12), p. 183.

6 Combining Blockchain and simple electronic time stamps

Blockchain technology can guarantee (under certain assumptions) that all changes to some data inserted in the past can be detected. The question arises whether this allows the construction of electronic time stamps. These are defined as “data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time” (Art. 3 no. 33 eIDAS regulation). Taking the Bitcoin blockchain as an example, inserting some data (like a photo of a rental car) into a block could establish that binding. Modifying that block at a later point in time is not technically impossible but requires a significant computational effort. We therefore assume that the presence of some data in a block of the Bitcoin blockchain does establish evidence that the data existed when the block was originally generated (i.e., the photo of the rental car showing some damage existed before the car left the car rental company’s premises). This evidence may not be irrefutable, but since security requirements are only introduced for qualified electronic time stamps, we assume that the evidence provided by a blockchain is sufficiently strong to qualify the blockchain as an electronic time stamp.

There is, however, an additional requirement. The data must be bound to a *particular* time. The Bitcoin blockchain has been constructed in such a way that a new block is generated, on average, every 10 minutes. There is a random element in the generation of blocks, so some blocks are generated more quickly, while others take longer. The average block creation time enables a rough estimate of the time a specific block was created.[22] Moreover, a (similarly imprecise) block time stamp is explicitly added to each block.[23] Other blockchains have similar properties to Bitcoin.[24] The time needed for block generation results in a delay. If it is important to prove that data have existed in a certain minute, the Bitcoin blockchain is therefore unsuitable.

When referring to a particular time, the eIDAS regulation does not make a statement concerning the required accuracy. As a link to the Coordinated Universal Time is an additional requirement for qualified electronic time stamps (Art. 42 (1) b eIDAS regulation), the Bitcoin blockchain (as well as similarly constructed other blockchains) provide simple electronic time stamps for the contained data.

This result is not very useful per se. There are few advantages to a simple electronic time stamp. Without a signature or seal provided by a qualified trust service provider—which is not normally contained in a blockchain—a qualified

[22] See Joseph Bonneau and Jeremy Clark and Steven Goldfeder, "On Bitcoin as a public randomness source" (2015) *Cryptology ePrint Archive*, available at https://eprint.iacr.org/2015/1015.pdf (accessed 22 July 2021).

[23] https://en.bitcoin.it/wiki/Block_timestamp (accessed 22 July 2021); for an example of a Bitcoin block, including the time of its generation (block time stamp) see https://www.blockchain.com/btc/block/00000000000000000000366a2127734056e9adce0e3161c1dae293d9a6df6eea4 (accessed 22 July 2021).

[24] E.g., for Ethereum, see Wood (n. 3) p. 5.

electronic time stamp cannot be achieved. We will therefore investigate, in the next step, how the two concepts can be combined.

7 Combining Blockchain and qualified electronic time stamps

As explained in Fig. 2, the usual technical procedure for generating secure time stamps (which may be used as qualified electronic time stamps) is simple. First the hash value of the content (e.g., photo of a rental car) is sent to a trusted third party, or a trust service provider (in the eIDAS terminology). Second, the trusted service provider appends the current date and time, signs the resulting data, and provides the result to its customer (see Fig. 2). For verification of the time stamp, all the data (original data, date and time, and the trust service provider) are required. In addition, signature verification requires the trust service provider's public key (or certificate, which contains that public key).

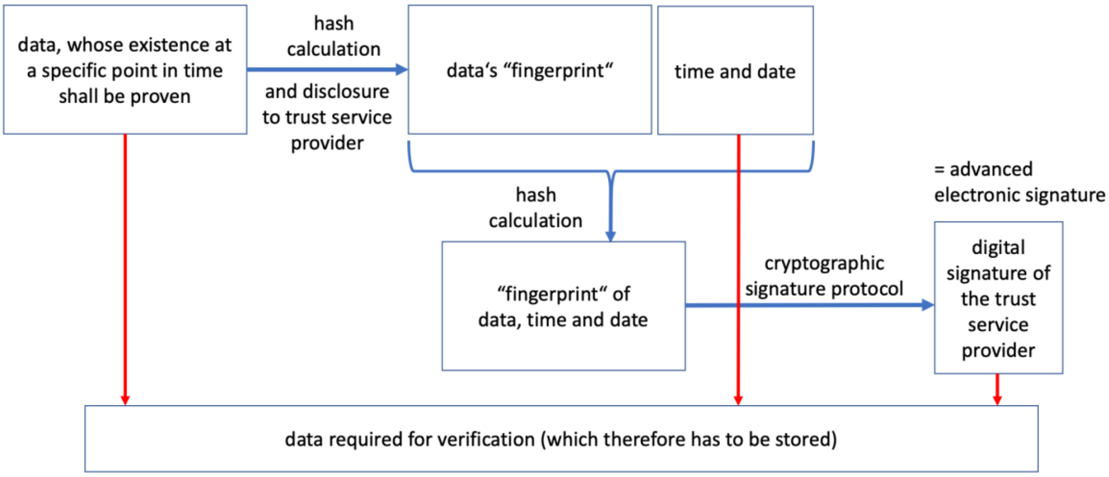
data, whose existence at a specific point in time shall be proven
hash calculation
and disclosure to trust service provider
data's "fingerprint"
time and date
hash calculation
= advanced electronic signature
"fingerprint" of data, time and date
cryptographic signature protocol
digital signature of the trust service provider
data required for verification (which therefore has to be stored)

Figure 2: Process for creating a qualified electronic time stamp (variations possible).

There is no relevant technical limit to the data that are time stamped. Instead of an individual file, one can compute the hash value of an entire blockchain block.

By sending the hash value to the trust service provider, one can receive a time stamp of that block (see Fig. 3). If the used hash function fulfils the security requirements specified in section 3, and a secure digital signature scheme is used, any modification of the block (and, consequently, of the individual document that has been added to the block) would be detectable. The argument can be extended. Even if only a hash value of a document is stored in the block, the time stamp proves that the document was in existence when the time stamp was generated.[25] Similarly, the root hash value of a Merkle tree can be used to prove the existence of any of the documents included in that tree.[26] Blockchains provide another advantage; as each block contains a hash value of the previous block, a time stamp of one block proves the existence of the previous block (and, by extension, the entire blockchain up to the block that is time stamped) at the time the time stamp has been generated. This may not be useful for very old blocks but may be relevant for the blocks generated within a few days before the time stamp was created. The time stamp may even be published, e.g., on the blockchain itself.

[25] This is based on the third additional requirement for cryptographic hash functions as described in section 3: It is not computationally feasible to find some other data that yields the same hash value (so-called property of collision resistance).

[26] See Katz and Lindell (*supra* n. 12) pp. 156, 183f.

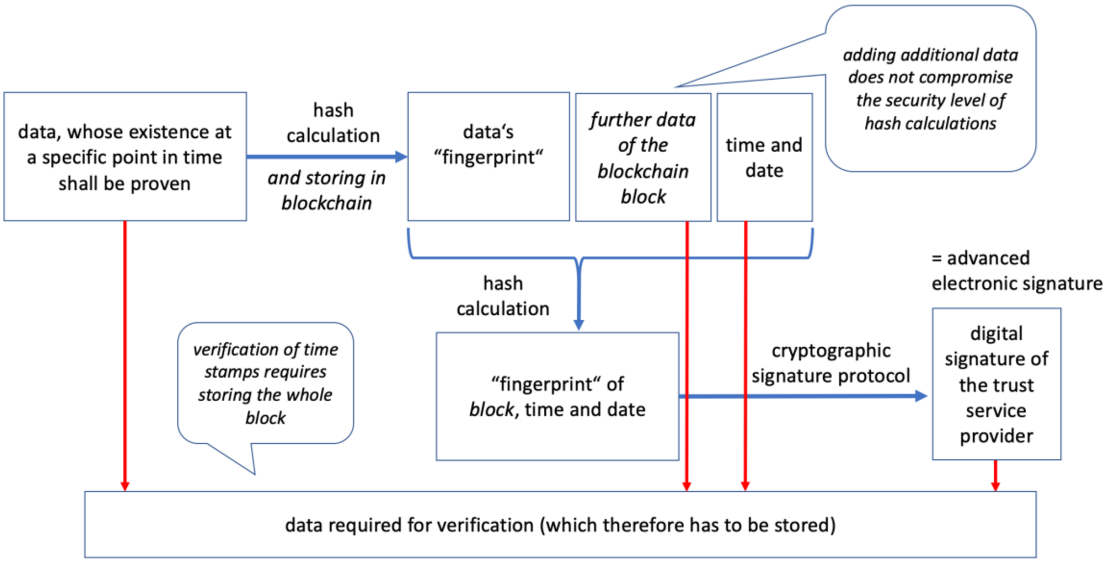
data, whose existence at a specific point in time shall be proven
hash calculation
and storing in blockchain
data's "fingerprint"
further data of the blockchain block
time and date
adding additional data does not compromise the security level of hash calculations
hash calculation
= advanced electronic signature
verification of time stamps requires storing the whole block
"fingerprint" of block, time and date
cryptographic signature protocol
digital signature of the trust service provider
data required for verification (which therefore has to be stored)

Figure 3: Process for creating a qualified time stamp—combined with Blockchain Technology.

If the trust service provider generates electronic time stamps based on hash values, there is no way to prevent customers from requesting time stamps for a blockchain block.

As a result, there are no technical restrictions to the application of secure electronic time stamps to a blockchain block, and by extension, the entire blockchain. However, the question arises whether this approach fulfils the requirements of the eIDAS regulation for qualified electronic time stamps. Art. 42(1) eIDAS regulation specifies three requirements. Two of those ((b) and (c)) only concern the trust service provider and the time source it uses. According to the third requirement, the time stamp must bind "the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably." We conclude that this is the case for the time stamp of a blockchain block generated according to Figure 3,[27] given the technical discussion above. This time stamp is a qualified electronic time stamp for all the blocks previously added to the blockchain—assuming the use of a secure blockchain, and a qualified trust service provider. However, the method as such is not currently standardized, which may impede its practical application. We therefore discuss to what extent the method deviates from existing standards that are part of the state of the art.

According to Art. 42(2), the eIDAS regulation empowers the European Commission to establish reference numbers of standards for the requirements defined in Art. 42(1)(a) and (b). This is supposed to happen by means of implementing acts. Where those standards are met, compliance with these requirements shall be presumed, therefore the electronic time stamp would be presumed qualified.[28] However, Art. 42(2) — as it is the case in several respective articles of the regulation[29] — only states that the European Commission *may* establish implementing acts. So far, this option has not been used.

This still means that a qualified electronic time stamp enjoys the presumption specified in Art. 41(2), regarding the accuracy of the date and time it indicates and the integrity of the data to which the date and time are bound. Nonetheless, the presumption regarding the requirements laid down in Art. 42(1) — meaning the presumption that the electronic time stamp is considered qualified — cannot be provided without the respective implementing act mentioned in Art. 42(2).

[27] Not to be confused with the block time stamp as specified for the Bitcoin blockchain (see section 6).

[28] Scaramuzzino, in: Zaccaria/Schmidt-Kessel/Schulze/Gambino (*supra* n. 10) Art. 42, para 3.

[29] See e.g. Art. 28 (6) regarding qualified certificates for electronic signatures or Art. 24 (5) regarding qualified trust service providers.

Despite these regulations, there are several ways to prove that the requirements to fulfil a qualified time stamp are met. According to recital 72, the European Commission is supposed to take due account of the (existing) standards and technical specifications drawn up by European and international standardisation organisation and bodies, when adopting implementing acts. Therefore, compliance with these standards and technical specifications can be used as indication that the requirements laid down in Art. 42(1) eIDAS regulation are met. Recital 72 particularly mentions the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU).

In fact, the ETSI Technical Committee Electronic Signatures and Infrastructures (ESI) has produced the European Standard ETSI EN 319 422, which specifies a "[t]ime-stamping protocol and time-stamp token profiles". In the following section we will analyse if the standard includes the requirements relevant for Art. 42 eIDAS regulation involving: specifications for the binding of date/time to data (a) and for accurate time sources (b). We focus on the core principles and omit implementation details.

7.1 Binding of date and time to data

The standard ETSI EN 319 422[30] provides a profile for the time stamping protocol defined in RFC 3161[31] (and the complementing standard RFC 5816[32]) of the Internet Engineering Task Force. This means that ETSI EN 319 422 limits some of

[30] ETSI EN 319 422 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

[31] RFC 3161: Internet X.509 Public Key Infrastructure–Time-Stamp Protocol (TSP).

[32] RFC 5816: ESSCertIDv2 Update for RFC 3161.

the options of the RFC.[33] The time stamping process corresponds to the one depicted in Fig. 2.

According to RFC 3161, the trust service provider (or "Time Stamp Authority", in the RFC's terminology) receives a hash value of the data to be time stamped—not the original data itself. It replies with a signature covering both the time stamped hash value, the current time (whose representation needs to include year, month, day, hour, minute and second) and an optional field specifying the accuracy of that time stamp. ETSI EN 319 422 requires the accuracy field to be supported. The standard also limits the choice of hash functions to those specified in clause A.8 of ETSI TS 119 312,[34] but states that this recommendation can be superseded by national recommendations. As a result, at least the hash function SHA-256 shall be supported. This hash function is quite common; in particular, the Bitcoin blockchain is based on SHA-256.[35]

It is obviously possible to send the hash value of a blockchain block to a trust service provider in accordance with ETSI EN 319 422. The provider will reply with a valid time stamp of the block. Our question, however, is: is this equivalent to a time stamp of any of the contents of the block, and of the previous block? At first glance, the answer seems obvious. If the block has existed at a certain point in time, so have its contents. However, for practical reasons, it would be helpful not to have to check the entire block—but, using the Merkle tree data structure, only some specific data. Moreover, if only a hash value of the original data is stored in the block, that means that a hash function has been

[33] ETSI EN 319 422, pp. 4-5.

[34] ETSI TS 119 312 V1.3.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[35] Nicolas Courtois and Marek Grajek and Rahul Naik, "Optimizing SHA256 in Bitcoin Mining" in Zbigniew Kotulski and Bogdan Księżopolski and Katarzyna Mazur (eds) *Cryptography and Security Systems* (CSS 2014, Communications in Computer and Information Science, vol 448, Springer, Berlin, Heidelberg), pp. 131-144.

applied more than once, which might not be in accordance with the standard. Consequently, a time stamp of a whole might not, at the same time, be a time stamp of its parts.

From a security perspective, however, neither additional hash calculations nor the use of a Merkle tree make a difference. As pointed out in section 5, a proper implementation of multiple hashing, or of a Merkle tree, provides the same security guarantees as the basic cryptographic hash function that is used. Fulfilling the same security guarantees means that the adapted approach (such as multiple hashing within a blockchain or combining the data to be hashed with other data in a Merkle hash tree) can be considered as a cryptographic hash function. On the other hand, any additional step not contained in the original standard defeats the purpose of providing a standardized verification procedure. In other words, a software based on the standards could verify the time stamp of a block but would not automatically link this time stamp to the individual contents of the block. Such a standardized procedure would be very helpful in practice. However, it is not required to achieve a qualified electronic time stamp according to Art. 42(1) of the eIDAS regulation so long as there is no implementing act based on Art. 42 (2) of the eIDAS regulation.

We conclude that our approach can, in fact, bind time and data to the data contained in a blockchain in a secure manner, fulfilling the requirements laid down in Art. 42(1) of the eIDAS regulation. It provides equivalent security to the relevant standards, which the European Commission could consider when passing an implementing act. Note, an explicit standardization of the approach would be helpful to enable practical adoption.

7.2 Accurate time sources

In principle, the selection of an accurate time source is a task for the trust service provider, no matter what data the time stamp is applied to. This does not change if an entire blockchain is time stamped, if one is aware that blocks may have been in existence long before the qualified time stamp was computed.

One might argue that using the blockchain in an intermediate step, instead of getting data time stamped directly, reduces the useful accuracy of the time stamp. RFC 3161 requires the "genTime" field, which states when the time stamp was generated, to include seconds. There is, however, an additional "accuracy" field, which specifies the possible deviation from the "genTime". The accuracy field, while optional according to the RFC, is mandated in ETSI EN 319 422, and needs to support a minimum accuracy of one second. Higher values, even in the order of hours or days, are not excluded by the standards. We still argue that the accuracy value, when used within our approach, should not reflect the delay between submitting data for inclusion in the blockchain, and generation of the time stamp. The semantics of the time stamp is evidence that data existed at a certain point in time—which may be determined, for example, with an accuracy of milliseconds or minutes. This does not preclude the existence of said data long before creation of the time stamp, whether they were included in a blockchain.

8 Long-term security

As explained in sections 3 and 5, security of the blockchain is based on technologies such as cryptographic hash functions, which need to fulfil certain requirements. If these requirements cannot be met in the long term, they may have a negative impact on the practicability of the blockchain. As a result, the method presented in the article at hand would no longer be considered as secure.

As an example, a cryptographic hash function may turn out not to be collision resistant (cmp. section 3). This is the case for the hash function MD5, which used to be very popular. In the case of MD5, so-called chosen prefix collision attacks made it possible to create hash collisions with practical relevance. Among others, researchers succeeded in creating forged digital certificates.[36] If similar attacks were found in the hash function on which a blockchain is based, this might allow an adversary to modify the existing blockchain. Depending on the precise properties of the attack, a replacement of entire blocks could well become possible.

Since the same issue exists for advanced electronic signatures (including qualified electronic signatures), methods to preserve their evidentiary value have already been standardized. Qualified preservation services, whose task is to ensure long-term security of qualified electronic signatures, are regulated in Art. 34 of the eIDAS regulation. The usual way to fulfil that task is to generate a qualified electronic time stamp, using a new (secure) digital signature scheme, which proves that the document with its original signature existed before an attack became feasible.

Insecurity of a hash function, however, cannot be mitigated as easily in a blockchain. Security of the entire chain depends on security of the hash function. Signing just the most recent block no longer proves the existence of the entire chain at a certain point in time if second-preimage resistance (or, depending on the type of attack, collision resistance) of the hash function is not guaranteed. Methods for transition to a new, more secure hash function have been described in literature.[37] However, these methods involve re-computation of hash values of past blocks. With the availability of qualified electronic time stamps, an alternative might include all past data from the blockchain in a new Merkle hash

[36] Marc Stevens et. al., "Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate" (2009) *Advances in Cryptology (CRYPTO 2009)* 55-69.

[37] Masashi Sato and Shin'ichiro Marsuo, "Long-term public blockchain: Resilience against Compromise of Underlying Cryptography" (2017) *26th International Conference on Computer Communication and Networks (ICCCN)* 1-8; Fengjun Chen et.al., "Secure Scheme Against Compromised Hash in Proof-of-Work Blockchain" in Man Ho Au et al (eds.) Network and System Security (NSS 2018, Lecture Notes in Computer Science, vol. 11058, Springer, Cham) pp. 1-15.

tree, based on the new hash function. A qualified trust service provider could then generate a time stamp of the root hash value. As hash values can be efficiently computed, and with a proof of work not being required in the "eIDAS world", the computational effort of this procedure would be manageable.

9 Possible economic consequences

Adoption of the scheme presented in this article is, however, not without risk. It implies that a single time stamp, issued by a qualified trust service provider, can be used to securely and reliably ensure that millions of documents existed at a certain point in time. This is possible by adding hash values of those documents to a blockchain and providing a hash value of the latest block to the trust service provider. There is no practical way for a trust service provider to prevent that use of his services. The only disadvantage for the users is a slight delay — potentially a few minutes — until a block is successfully added to the chain, and the time stamp is computed.

A consequence of this is it creates an economic problem. For most users, a blockchain-based time stamp fulfilling the eIDAS requirements of a qualified electronic time stamp is likely sufficient, so there is little incentive to pay the trust service provider for individual time stamps. As a result, trust service providers might decide to stop providing time stamp services, except when needed for other business (such as qualified preservation services, Art. 34 eIDAS regulation). Should such a situation arise, a reaction by the states (e.g., by providing a state-sponsored blockchain that includes qualified electronic time stamps) might make sense. Such infrastructure could also play an essential role for the long-term preservation of the evidentiary value of electronic signatures, making qualified preservation services (cmp. section 8) obsolete. This result seems to contradict the approach of the eIDAS regulation, which generally assigns the role of trust service providers to typically private, competing market players. Note, however, that other trust services, particularly those related to electronic signatures, would not be affected.

10 Commission proposal for amending the eIDAS regulation

A recent proposal by the European Commission[38] contains regulation concerning the concept of electronic ledgers, amending the eIDAS regulation. The proposal includes the following definition:[39]

> 'electronic ledger' means a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering.

Furthermore, the proposal contains a new section[40] for the eIDAS regulation, which specifies — comparable to other trust services — regulations about the legal effects and requirements for (qualified) electronic ledgers.

A *qualified* electronic ledger must be created by at least one qualified trust service provider. It must ensure the correct sequencing of data entries recorded in the ledger as well as the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry. Furthermore, it must record the data in such a way that any subsequent change to the data is immediately detectable.[41] The legal effect of qualified electronic ledgers is laid down in Art. 45h(2) according to the proposal:

[38] Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, 2021/0136 (COD), 03.06.2021.

[39] See p. 23 of the proposal (Art. 3 no. 53).

[40] See p. 41 of the proposal (Art. 45h and 45i).

[41] See p. 41 of the proposal (Art. 45(i))

> A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger.

Overall, this concept of electronic ledgers has some similarities to the concept discussed in this article, and a blockchain could serve as a technical basis. However, such a qualified electronic ledger must be created by an electronic trust service provider, and authenticity of the data needs to be ensured. In the article at hand, we focus on the pure proof of existence of data at a certain point in time. The involved trust service provider, which only provides a time stamp, need not even be aware of the existence of the blockchain.

Due to the ongoing discussion, the final version of the proposed amendment might differ from the version presented here. Currently, there is no reason to assume that an amended eIDAS regulation will have an impact on the technical or legal considerations in the article at hand.

11 Conclusion

Electronic time stamps have received little attention in the legal literature so far, but may be very helpful in practice — e.g., to secure evidence in IPR matters or to document the condition of a rental car. A simple smartphone app could upload the hash value of photos or videos to a time stamping service, thereby creating evidence about the condition of the rental car at (or before) a specific time. Blockchains can be used to realize electronic time stamps, but their use in court may be inefficient despite their technical properties, as there is no central operator to guarantee their correctness.

Using the method presented in this article, the best of both worlds may be achieved: the "eIDAS world", which is based on the use of regulated trust service providers, and the "blockchain world", which is based on a decentralized trust model, and is supposed to make participation quick and easy. Note that consensus mechanisms, which are used to decide which data are added to a blockchain, are an important aspect of blockchain technology — but our approach is largely independent from them. In its core, the approach relies on the existence of a data structure, such as a Merkle tree, that fulfils the requirements of a cryptographic hash function and allows the computation of a "fingerprint" covering an arbitrary amount of documents (or other data). In fact, the use of such data structures in combination with time stamps has already been standardized.[42] Use of a blockchain may, however, have practical advantages — e.g., because they provide distributed storage.

Acknowledgement

This research was supported by the "EVAREST" project as part of a strategic individual grant from the German Federal Ministry for Economic Affairs and Energy (grant reference: 01MT19003E). Further information on the research project can be found at www.evarest.de.

[42] RFC 4998: Evidence Record Syntax (ERS).