USAGE SCENARIOS FOR BLOCKCHAIN TECHNOLOGIES IN THE DOMAIN OF CIVIL LAW NOTARIES

Hans-Georg Fill and Felix Härer

Abstract: Blockchain technologies have recently been discussed also in regard to their application in the legal domain. In this paper we take the perspective of civil law notaries as an established and trustful institution and derive two potential usage scenarios for using public permissioned blockchains in this area. Thereby, the specificities of civil law notaries as state-appointed officials who provide independent, impartial and objective advice for important legal transactions need to be considered. The usage scenarios intend to show possible directions for future blockchain applications.

Table of contents

A. MOTIVATION

In many domains blockchain technologies are currently being explored for bringing benefits for the trustful, decentralized, and transparent storage of information and the decentralized processing of information via so-called smart contracts. Recent examples for successful applications can be found e.g. in the domain of logistics with the TradeLens blockchain for tracking cargo, which is developed by the companies IBM and Maersk (TradeLens 2019), the Bloxberg blockchain for scientific publications initiated by Max Planck Institute (Vengadasalam et al. 2019), or the availability of blockchains-as-a-service by Amazon Web Services for easily setting up one's own blockchain (Amazon 2019).

Furthermore, blockchain technologies are investigated for running public registers, e.g. for leading to more transparency in countries with inefficient and intransparent land registration systems or for enhancing government services such as identity management, electronic voting systems or the attestation of certificates through the provision of immutable storage that is not managed by a central authority (Ølnes et al. 2017).

Thereby it is often argued for disruptive changes by replacing existing processes with blockchain-based solutions (Lansiti and Lakhani 2017). The idea behind is to make processes more efficient in terms of cost and time by replacing traditional intermediaries with algorithmic agents that autonomously decide about the steps for recording information on immutable, decentralized registers, e.g. (Seeber et al. 2018). Although this direction seems appealing, the amount of expertise required for conducting such processes is mostly underestimated c.f. (Barbieri and Gassen 2017). For example, in the domain of legal consulting by sovereign civil law notaries, which is obligatory in many countries for processes such as property transactions or the issuance of patient decrees due to the high stakes and numerous risks involved, profound legal expertise is necessary (Woschnak 2005). In addition, civil law notaries have to observe requirements such as the obligation to respect all interests of involved parties, be impartial and treat all issues objectively. It has been shown that this type of preventive justice by notaries leads in general to lower public legal expenditures per capita (Helmenstein 2016).

Although approaches developed in the field of artificial intelligence may in the future be able to master certain tasks in legal consulting, the state of current systems still shows

deficiencies in human abilities that are essential in this domain such as general world knowledge, emotional intelligence, creativity, common sense reasoning, adaptability or responsibility cf. (Woschnak 2018, Dellermann et al. 2019). The approaches based on machine learning that currently dominate the field of artificial intelligence are rather able to learn patterns from previous cases and then apply these patterns in a useful way. The judgement of these outcomes, for example from an ethical perspective, is an active area of research. Recently presented approaches in regard to «Responsible AI» only touch the surface of this complex topic, cf. (Dignum 2018). With recent developments towards so-called «Hybrid Intelligence», it is thus rather aimed for solutions that focus on a cooperation between humans and artificial intelligence where both parts can learn from each other and complement their specific capabilities (Kamar 2016; Dellermann et al. 2019).

The idea of hybrid intelligence can be applied in a similar fashion to the field of blockchain technologies where synergies between these technologies and humans may be investigated. It thus seems worthwhile to come up with designs where blockchain-based systems and humans work in cooperation similar to the concept of Hybrid Intelligence. This may not only increase the transparency of transactions but lead to entirely new types of solutions.

In this paper we illustrate how this direction can be applied to the domain of civil law notaries. As has been shown in the past, notaries are active users of digital technologies and can contribute to high security requirements, e.g. for attesting not only the physical identity but also aspects such as the accountability, the will and contractual capability of a person when he/she signs a contract cf. (Collantes 2017). First attempts for integrating notaries and blockchain technologies have been recently presented in a paper at the BPM blockchain forum where notaries and other parties are connected via blockchain technologies for conducting land registrations (Fernando and Ranasinghe 2019). For this purpose, we describe two usage scenarios that show how blockchain technologies can be used in an innovative way for supporting notaries and offer new solutions for their clients. The aim of this contribution is to illustrate how blockchain technologies could be integrated in civil law notaries' processes.

The paper is structured as follows: in section B we will briefly discuss the foundations of blockchains and smart contracts. The usage scenarios will then be described in section C, which is followed by a discussion and an outlook.

B. FOUNDATIONS

In this section we briefly describe the foundations of blockchains and distributed ledger technologies as well as smart contracts. For more detailed elaborations we refer to the introductory literature (Fill and Meier 2020). Concerning the characterization of blockchains we mainly refer to the concepts as used for the Bitcoin blockchain (Nakamoto 2008) and for describing Smart Contracts to the specifications used for Ethereum (Buterin 2013; Wood 2014).

I. Blockchains as Distributed Ledgers

Blockchains are one form of so-called electronic distributed ledgers. The term stems from the data structure that is used to store information: A block may contain one or several transactions that stand for transfers of value, tangible or intangible properties. Each transaction is electronically signed by an actor using his/her private key of a public-private key pair. This permits to trace transactions and ensure that only the actors who are authorized can use their resources for transactions. In addition to the transactions, each block is assigned a timestamp and a reference to the previous block. This reference contains a hash value of the data of that previous block, thus chaining the blocks together. If the data in the previous block or any of its predecessors would change, also that hash value would change thereby indicating a breach of the immutability principle of blockchains. Copies of the blockchain are held by numerous parties in a peer-to-peer network. This means that there is no central instance governing the blockchain but rather a network of peers who constantly monitor the blockchain.

For adding transactions to the blockchain, an actor needs to send a signed transaction to its neighbouring peers who then forward the transaction to their peers and so on. In order to avoid misbehaviour of any of the peers in the network, public blockchains use a specific type of consensus mechanism for deciding which of the peers is permitted to add a new block with transactions to the chain. In Bitcoin, this is for example achieved by proof-of-work (Narayanan et al. 2016), the Blockchain's so-called cryptographic puzzle that needs to be solved by all participating nodes. These puzzles contain computationally hard exercises that can only be solved by investing computational resources in a brute-force manner. Once a participant finds a solution – which is determined by

chance in proportion to the resources invested – this participant is selected and permitted to add a new block to the blockchain. The new version of the blockchain is then forwarded to all peers who verify the contained information and the correct resolution of the puzzle. In this way, no participant is given preference to the other peers and all transactions on the blockchain are fully transparent.

Whereas public blockchains are open for anyone to read and write data to them based on the consensus protocol, the access to blockchains may also be restricted (Xu et al. 2017) – see Figure 1. We thus distinguish between *Permissionless Public Blockchains* where everyone can read and write data to the blockchain, *Permissioned Public Blockchains* where the contents can be inspected by anyone but the write access is restricted to particular persons and *Permissioned Private Blockchains* where both read and write access are restricted. The main advantage of public readability is, especially in comparison to distributed databases or websites, public verifiability. Anyone is able to validate the correctness of data, specifically its integrity and whoever recorded it in terms of digital identities and signatures.

	Public Readability	*No Public Readability*
Public Write Access	**Permissionless Public Blockchains**	
Controlled Write Access	**Permissioned Public Blockchains**	**Permissioned Private Blockchains**

Figure 1: Types of Blockchains

Thereby, permissionless public blockchains are typically developed by the open-source community. In case of intentional updates or unintentional bugs in the corresponding software implementations, it may occur that new versions (hard forks) of the blockchain are not downward compatible – see for example the hard fork of Ethereum (Etherchain 2019; Mehar et al. 2019). In cases with only minor updates to the blockchain protocol, it can be made more specific such that new versions take advantage of new features while old versions are still compatible (soft fork) – see for example the Segregated Witness soft fork in Bitcoin (Lombrozo et al. 2018). From an enterprise perspec-

tive, this type of blockchain thus carries an inherent incompatibility risk and thus potential costs for the migration to a new version if this is possible at all. In addition, permissionless blockchains today typically rely on the proof-of-work consensus protocol that is very energy consuming.

Permissioned blockchains can overcome some of these disadvantages. Due to the restricted access, the evolution of the software basis can be done in a controlled fashion so that downward compatibility is guaranteed or that appropriate migration strategies can be conceived. They can still offer transparency, even to the public and do not require the excessive amounts of energy as permissionless blockchains. This type of blockchain is therefore intensively explored for industrial applications at the moment.

II. Smart Contracts

In addition to storing transactions for the exchange of value between the blockchain's participants, smart contracts permit algorithms to be executed. A smart contract is specified as program code in a way suitable to store and execute it on a blockchain. The execution is performed in a decentralized fashion, i.e. the smart contract code is run (1) distributed on the nodes of a network and (2) interpreted according to the protocol of the blockchain (Wood 2014).

From the perspective of a participant, a smart contract is stored by sending a transaction with the smart contract code to the network where an address is assigned. The execution is invoked by sending a transaction to the address, calling the smart contract at a specific function (Antonopoulos 2018). Smart contracts can achieve decentralization in storage and execution regarding the architecture of the system out of distributed nodes run by participants and the coordination of the non-centralized execution.

In this way, smart contracts can be used as decentralized applications which augment the traditional computer software application with specific properties of blockchains (Xu et al. 2017; Böhme and Pesch 2017). In the following, immutability, deterministic execution and transparency of smart contracts are discussed with relevant applications.

Smart contracts are immutable as once they are stored, they cannot be overwritten or changed. This immutability property applies to the contract code as well as to data that the contract may store as a result of its execution. An application for this property is

attestation, i.e. the assertion made by a smart contract that a document exists and has not been changed. Given the document, the corresponding integrity data is computed based on its content and compared to the value stored in the smart contract c.f. (Härer and Fill 2019). The block in the blockchain which contains the data provides a timestamp of the attestation.

Smart contracts are sometimes attributed with the ability of impartially evaluating machine-processable legal contracts due to the possibility of deterministic execution. Deterministic execution is a property asserting that multiple executions of contract code always result in the same outcome, given equal data as input. Notably this property holds true for the distributed nodes of the network, since all nodes interpret contract code according to the protocol of the blockchain. Before the execution of contract code starts, the blockchain with all state variables is synchronized across all nodes providing for equal data. The execution interprets the contract code according to the blockchain protocol equally on all network nodes resulting in the same values of state variables after the execution. While this property can be applied to machine-processible conditions, this notion carries obvious limitations when it comes to legal contracts functioning on the basis of real-world scenarios rather than data.

The transparency property concerns the possibility to observe all smart contract code and data stored in state variables as well as to validate the outcome of previous smart contract executions. In blockchains with public read access, the general public is able to inspect smart contracts. Because of immutability, any participant possesses the same integrity-secured set of blocks defining the current execution state of all smart contracts. Due to deterministic execution, the nodes of participants execute smart contracts and validate whether the outcome matches the state variables present in blocks. This step occurs for each newly propagated block automatically in order to ensure the correct interpretation of smart contract executions according to the protocol of the blockchain. In certain settings, however, public readability might not be desired and achieved by encryption or private blockchains or databases.

In spite of transparency, smart contracts in public and private blockchains may restrict write access to the data they control. Since participants interacting with the contract are known by their public key or a derived address, a contract can contain conditions for checking whether the execution is invoked by an authorized participant. Access

control schemes may, for example, allow for the transfer of tokens between multiple addresses previously authorized by the creator of the smart contract.

C. DESCRIPTION OF USAGE SCENARIOS

The usage scenarios we will describe in the following are based on a public permissioned blockchain that is maintained by the civil law notaries of a country. It will thus be denoted as a «Notary Blockchain» in the following. For participating in the blockchain it is assumed that the initial set-up is conducted by the chamber of notaries or a similar body which oversees the appointment and withdrawal of notaries and issues and withdraws permissions for the write access to the blockchain. Other actors such as citizens and other government bodies then receive access through the notaries. These access rights are transparently stored on the blockchain. The nodes of the blockchain are operated by any authorized notary in a country for ensuring transparency and the distributed, secure storage of information.

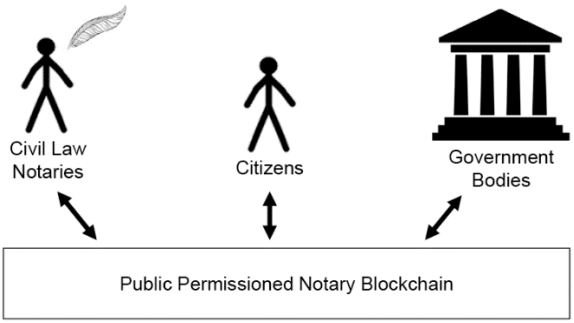

Figure 2: Actors in the Context of a Notary Blockchain

Based on this Notary Blockchain two usage scenarios will be described: the issuing of temporal digital identities and the notary-based attestation of the signing of documents. The main advantage in regard to traditional distributed database approaches is thereby the full transparency of information towards all involved parties and the additional security and legal consulting contributed by civil law notaries.

I. Issuance of Temporary Digital Identities via a Notary Blockchain

The idea for this usage scenario stems from the fact that the use of qualified electronic signatures and electronic identities becomes more and more common in Europe. Especially, the forthcoming ubiquitous availability of electronic IDs (eIDs) will open new possibilities for authenticating people both online and offline (Popolari 2019). Such eIDs will be issued by governments for their citizens and are expected to replace traditional paper-based identification documents such as passports or identity cards. Depending on how eIDs are implemented in practice, the possibility exists that the personal data can be traced across several applications and platforms, both by companies as well as government bodies.

However, it would be beneficial to prove the existence of an identity without actually disclosing the personal data. In the real world this would correspond to showing an ID document that can be inspected and verified. At the same time, it is however prevented that someone copies the data on the document. For realizing such a scenario, different options are available. One option would be to revert to cryptographic schemes that permit to check the validity of an eID without having to give away the personal data. The authority issuing the eID could thus sign a specific part of the eID with its electronic signature, e.g. a unique identification number that cannot be related to a person. This signature could then be presented to a third party who can verify the signature using the certificate of the issuing government authority. In this case, the holder of the eID would remain anonymous – however, if the unique identification number is recorded, the issuing government authority could still trace the holder as she knows who stands behind the identification number.

By introducing civil law notaries in this process, an additional level of security could be added. The main idea is that notaries – as sovereign but independent actors in the judicial system – could issue temporary digital identities that are fully anonymous. A notary would thereby guarantee for the correctness of the issued identity and attest that it relates to an actual physical person, the citizen. Based on the high confidentiality requirements for notaries, they would keep the linkage between the anonymous identity and the real identity in a highly secure place, e.g. their office safe where the most

sensitive documents of clients are stored offline. The anonymous identity can then be used by its holder just as a standard electronic identity but without containing any identifying information. If necessary, additional attributes could be added to this anonymous identity, e.g. the age of a person or the nationality – which may be useful for a range of online services that are restricted to certain age groups or national boundaries. In this way it would be prevented that personal information can be traced across service interactions over time, even by government authorities. These relationships are shown in Figure 3.

If, however, the citizen misuses the anonymous identity, e.g. for committing crimes, a prosecutor could demand from the notary – typically based on a warrant issued by a judge – to disclose the linkage between the anonymous identity and the real person.

For realizing such a scenario, blockchain technologies could be beneficial. In particular, a notary blockchain could be used to store the information about the attested anonymous ID and revoke it if necessary. The notary blockchain would be regarded as a trusted source of information where information on the anonymous identities can be retrieved. Dedicated signature servers would not be required. Due to the decentralized and distributed nature of this blockchain, the information would not be held at one place but distributed over all nodes of the blockchain.

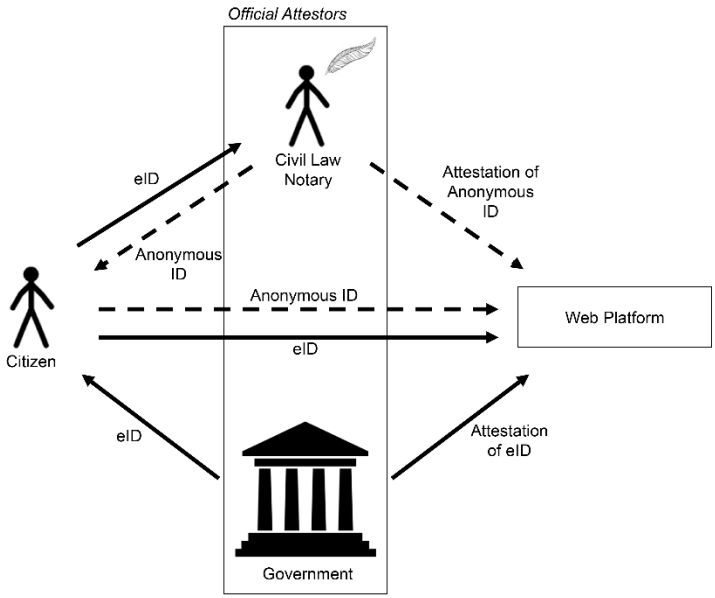

Figure 3: Issuance of Anonymous IDs Through Notaries

This would increase fault tolerance. As the blockchain is publicly accessible, full transparency of all transactions would be ensured. Citizens could even self-manage their anonymous identities on the blockchain using smart contracts, e.g. for requesting a new anonymous identity once it has expired. The strict separation between the actual electronic identities and the anonymous, notary-issued identities would prevent the collection of personal data by other parties. If multiple anonymous identities are issued per citizen, even the correlation of actions based on a particular identity, e.g. on different web platforms, would not be possible.

For realizing such a scenario in practice, a number of additional aspects would need to be considered. For example, it would need to be investigated, whether the costs of operating such an infrastructure would outweigh the benefits for citizens of disposing of anonymous identities.

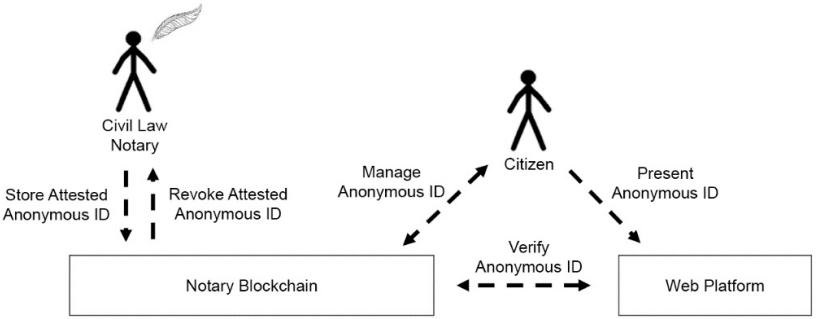

Figure 4: Managing Anonymous IDs Using a Notary Blockchain

Further, the feasibility of a technical realization would need to be evaluated using a proof-of-concept. Thereby it would need to be evaluated whether existing software platforms for blockchains could be re-used or would need to be adapted. Finally, as for any software solution, potential security risks would need to be assessed and mitigated.

II. Attestation of the Signing of Documents by Notaries Using Blockchains

The notarial attestation of the act of signing documents is a central service provided by civil law notaries. The involvement of notaries institutionalizes these tasks for the benefit of individuals and organizations, ensuring the identity every time a document is signed, the existence and awareness of a document's contents and the validity of the signature. In addition, it is checked every time and for every case whether the signing party has the necessary legal capacity (German: Geschäftsfähigkeit), that the parties are prevented from acting with undue haste (German: Übereilungsschutz, «frei von Zwang»), and that anti-money laundering and counter-terrorism regulations are satisfied – in Austria the details on this procedure are regulated in the Sections 79 as well as 34 and 36a-f of the Austrian Law on the Notarial Profession (§ 34, § 36a-f NO). These assertions are provided to third parties when presenting documents with notarial certifications, in a legally binding manner.

In the following we thus explore the possibility of enhancing the notarial attestation of signing documents in front of a notary with the possibilities of storing this attestation

using a blockchain. In this way, the validity of an attestation can be electronically verified by accessing the public record of a blockchain, where the validity of attestations and of keys used by notaries can be established in a decentralized manner, i.e. no centralized public-key-infrastructure is required. At the same time, the role of the notary is to ensure the properties for the status of the involved parties from above that have to be checked.

Technical solutions for blockchain-based attestation have been suggested early on (Kirk 2013), now including approaches for existence and integrity assertions (Crosby 2016), decentralized identity management (Simons 2018), the attestation of documents (Swan 2015) and conceptual models and ontologies (Fill 2019; Härer and Fill 2019; Fill and Härer 2018). In these approaches, the integrity data of an artifact is created solely based on its content, usually by processing it with a hash function. This function produces a fixed-length output, which summarizes the document's contents. Any change of the document results in an unpredictable change of the hash value. Thus, attestation approaches usually (1) create a hash value of a document, and (2) store the hash value in the blockchain. For verifying the prior existence of the document, (3) any third party in the possession of the document is able to reproduce its hash value and (4) compare it to the value stored in a previous block by executing a smart contract. The existence of the document is established for the timestamp of the block. Notably, technical attestation solutions so far do not consider the additional properties provided through the involvement of civil law notaries. This concerns in particular the ensuring of the real physical identity of a person, the legal capacity of the person, that the parties are acting with undue haste as well as the satisfaction of anti-money laundering and counter-terrorism regulations.

The ensuring of these latter properties not only requires profound legal knowledge, e.g. concerning the various legal regulations underlying this process, but also abilities that can today not be substituted by machines such as general world knowledge, common sense reasoning, adaptability or responsibility. For example, it depends on the particular physical condition of a person and its personal behaviour to assess whether a person has the legal capacity to know about the contents of an important document and is not forced to sign it by other parties or circumstances. AI systems may in the future be able to acquire these human abilities and act in an ethically responsible way – but today they

are not capable of performing them. Therefore, the human in this process could not be eliminated using digital means. However, it may be possible to enhance the process through digitalization in the sense of hybrid intelligence described in the introduction, where humans and machines complement each other. This could also be the case when introducing the technology of blockchains in this process. Before we can discuss this, we have to review however, which electronic means are already used in this context today.

The process of the attestation of the signing of documents is already today supported by the use of electronic signatures. Here, (1) a document and its integrity data are signed in front of a notary using a key from the qualified certificate of a citizen, possibly stored on an electronic ID card proving the identity of the signer. (2) Another signature is applied by the notary using the specific certificate issued to them as part of their sovereign power – for the details see section 47 of Austrian Law on the Notarial Profession (§ 47 NO). For the creation of integrity data, a process similar to the one described for attestation is used. While an electronic signature binds a document to an identity in a non-repudiable manner, it relies on the availability of the correct issuance of certificates. Notaries are provided with electronic signatures that are issued by a trusted service provider such as A-Trust in Austria (BMVRD 2011) or the German Chamber of Notaries (Bundesnotarkammer 2019). Although the issuance and revocation of certificates are strictly regulated by law, it can today not be easily checked by the general public which signature is valid or has been valid at a certain point in time.

The suggestion for a hybrid solution therefore consists of two components. (1) Issuance and revocation of certificates through a notary blockchain and (2) augmenting the attestation of the signing of documents with the option of storing the attestation information on a blockchain so that third parties can verify this information. The concept is described in Figure 5.

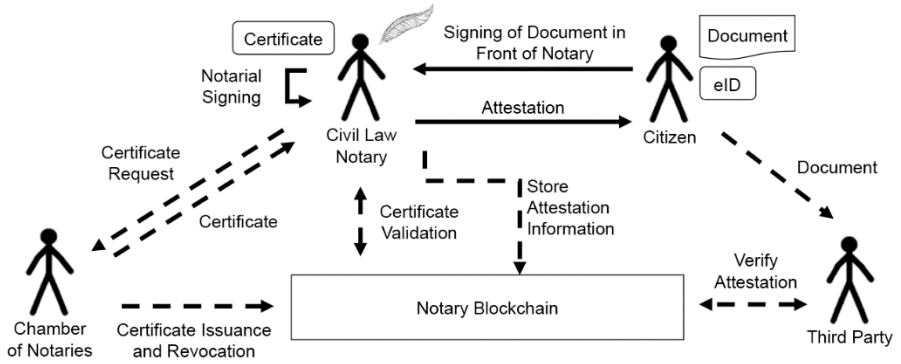

Figure 5: Notarial Attestation of Signing Documents Using a Notary Blockchain

In (1), the Civil Law Notary requests a certificate from the Chamber of Notaries as a trusted service provider. The issuance, however, consists of storing the certificate's public key on the notary blockchain, where its validity can be checked by any party, and returning the certificate to the notary. Thus, a certificate is only valid if it can be found and verified on the blockchain.

For (2), a document and an eID held by a citizen are presented to the notary as common today. That is, the civil law notary validates all properties required for a notarial attestation and ensures the correct signing of the document by the Citizen. For reading the eID and for placing the signature, the process is carried out in a controlled environment using specific devices, e.g. a certified card / NFC reader for eIDs. Subsequently, the document is also electronically signed by the notary and either returned or stored. Attestation information consisting of the electronic signature only is returned to the citizen and stored on the notary blockchain. In this case, a third party can verify the correctness of the signature by consulting the blockchain.

The issuance of certificates on the blockchain has the advantages of transparency, availability, and traceability over time. Each certificate issuance and also each revocation is recorded and documented on the blockchain in an immutable manner and with a dedicated time stamp. It can be transparently inspected by everyone and copies of the blockchain can be stored by anyone in a decentralized way. This directly contributes

also the idea of open government processes. In addition, the complete ledger of previous certificates is available. In this way, certificates issued previously are still verifiable. In the case of a revocation, the validity period of the certificate is documented and verifiable. This is important especially for long-lasting documents whose contents may be verified after several years when today's certificates have already expired and the issuing notary may have retired.

D. CONCLUSION AND OUTLOOK

From a technological point-of-view, the immutable storage and verifiable execution of data can be facilitated by blockchain technologies. While there is clearly technical advancement which merits the discussion of these topics on their own, the complexity of the underlying domain of civil law notaries is usually underestimated. Often, notaries are regarded only as intermediaries for attestation and signature-based authorization. In this view, the scope of activities of civil law notaries is disregarded, neglecting their impartial, independent, and objective function for legal consulting under the obligation to respect all interests of the parties involved as well as their obligation to ensure that transactions are conducted only by legally competent parties with undue haste and by respecting anti-money laundering and counter-terrorism regulations. They are appointed by a state as trusted third parties with the highest confidentiality obligations and possess ample experience in complex legal cases for citizens and companies alike. Blockchain technologies may complement this traditional role of civil law notaries as has been shown using the usage scenarios of anonymous identities and of the attestation of the signing of documents by notaries.

Although first ideas could be sketched in this contribution, the actual development of systems where civil law notaries can make use of blockchain technologies clearly requires further research and the implementation of proof-of-concept solutions. This would permit to engage in further evaluations and a refinement of the necessary requirements for such solutions.

ACKNOWLEDGEMENT

We would like to thank Mag. Katharina Haiden-Fill MBL for giving us insights into the domain of civil law notaries and for pointing us to the relevant legal regulations.

REFERENCES

Amazon (2019): Amazon Managed Blockchain – Management Guide, URL: https://docs.aws.amazon.com/managed-blockchain/latest/managementguide/managed-blockchain-mgmt.pdf (Accessed 2019-10-04).

Antonopoulos, A. M. (2018): Mastering Ethereum: Building Smart Contracts and Dapps, OReilly Media.

Barbieri, M., Gassen, D. (2017): Blockchain – can this new technology really revolutionize the land registry system?, Paper prepared for presentation at the 2017 WORLD BANK CONFERENCE ON LAND AND POVERTY, The World Bank – Washington DC, March 20–24, 2017.

BMVRD (2011): Bundesminister für Verfassung, Reformen, Deregulierung und Justiz: Anwendungen der österreichischen Justiz für Notare, URL: https://sv.justiz.gv.at/edikte/welcomereg.nsf/nol/z1 (Accessed 2019-10-04).

Böhme, R., Pesch, P. (2017): Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, Datenschutz und Datensicherheit – DuD, Volume 41, Issue 8, p. 473–481.

Bundesnotarkammer (2019): Zertifizierungsstelle der Bundesnotarkammer, URL: https://zertifizierungsstelle.bnotk.de/ (Accessed 2019-10-04).

Buterin, V. (2013): Ethereum: The Ultimate Smart Contract and Decentralized Application Platform, URL: http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html (Accessed 2019-10-04).

Collantes, José Manuel Garcia (2017): Start-Ups und Notare, in: Schnauder, Andreas (Eds.): Digitalisierung im Gesellschaftsrecht – Chancen und Risiken, Schriftenreihe des österreichischen Notariats, Band 61, Manz, S.103.

Crosby, M. (2016): BlockChain Technology: Beyond Bitcoin, Applied Innovation Review, Issue 2 2016, p. 16.

Dellermann, D., Ebel, P., Söllner, M., Leimeister, J.M. (2019): Hybrid Intelligence, Business & Information Systems Engineering, Volume 61, Issue 5, p. 637–643.

Dignum, V. (2018): Ethics in artificial intelligence: introduction to the special issue, Ethics and Information Technology, Volume 20, Springer.

Etherchain (2019): Ethereum Hard Fork History, URL: https://www.etherchain.org/hardForks (Accessed 2019-10-04).

Fernando, D., Ranasinghe, N. (2019): Permissioned Distributed Ledgers for Land Transactions; A Case Study, in: Di Ciccio, C., Gabryelczyk, R., García-Bañuelos, L. (Eds.): Business Process Management: Blockchain and Central and Eastern Europe Forum, Springer, p. 136–150.

Fill, Hans-Georg (2019): Applying the Concept of Knowledge Blockchains to Ontologies, in: A. Martin, K. Hinkelmann, A. Gerber, D. Lenat, F. van Harmelen, P. Clark (Eds.), Proceedings of the AAAI 2019 Spring Symposium on Combining Machine Learning with Knowledge Engineering (AAAI-MAKE 2019). Stanford University, Palo Alto, California, USA

Fill, H.-G., Härer, F. (2018): Knowledge Blockchains: Applying Blockchain Technologies to Enterprise Modeling, HICSS'51, AIS, pp.4045–4054.

Fill, H.-G., Meier, A. (2020): Blockchain kompakt – Grundlagen, Anwendungsoptionen und kritische Bewertung, Springer.

Härer, F., Fill, H.-G. (2019): Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain, 21st IEEE International Conference on Business Informatics (CBI 2019).

Helmenstein, C. (2016): Die Vorteile einer vorsorgenden Rechtspflege für die Effektivität von Justizsystemen, in: Helmenstein, C. (Eds.): Wert plus Mehrwert. Für Mensch und Wirtschaft – Vorsorgende Rechtspflege in Europa, Schriftenreihe des österreichischen Notariats, Band 57, Manz, S.13–20.

Jun, M. (2018): Blockchain government – a next form of infrastructure for the twenty-first century, Journal of Open Innovation: Technology, Market, and Complexity, Volume 4, Issue 1, p. 7.

Kamar, E. (2016): Hybrid workplaces of the future, XRDS: Crossroads, The ACM Magazine for Students – The Future of Work, Volume 23, Issue 2, ACM, p. 22–25.

Kirk, J. (2013): Could the Bitcoin network be used as an ultrasecure notary service?, Computerworld, URL: https://www.computerworld.com/article/2498077/could-the-bitcoin-network-be-used-as-an-ultrasecure-notary-service-.html (Accessed 2019-10-04).

Lansiti, M., Lakhani, K. R. (2017): The Truth about Blockchain, Harvard Business Review, Volume 95, Issue 1, p. 118–127.

Lombrozo, E., Johnson, L., Wuille, P. (2018): Bitcoin Improvement Proposal 141, URL: https://github.com/bitcoin/bips (Accessed 2019-10-04).

Mehar, M. I. et al. (2019): Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack, Journal of Cases on Information Technology (JCIT), Volume 21, Issue 1, p. 19–32.

Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, URL: https://bitcoin.org/bitcoin.pdf (Accessed 2019-10-04).

Narayanan A., Bonneau J., Felten E., Miller, A., Goldfeder, S. (2016): Bitcoin and Cryptocurrency Technologies, Princeton University Press, Princeton.

Ølnes, S., Ubacht, J., Janssen, M. (2017): Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly, Volume 34, Issue 3, p. 355–364.

Popolari, M. (2019): Umsetzungsprojekt Sicheres Identitätsmanagement, A Trust Innovation Day 2019, URL: https://www.a-trust.at/MediaProvider/2448/innovation-day-2019_e-id_popolari.pdf (Accessed 2019-10-04).

Seeber, T., Schweiger, M., Schachner, M. (2018): Immobilientransaktionen über die Blockchain, immolex, Februar 2018, p. 38–42.

Simons, A. (2018): Decentralized digital identities and blockchain: The future as we see it, Microsoft, URL: https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/ (Accessed 2019-10-04).

Swan, M. (2015): Blockchain: Blueprint for a New Economy, OReilly Media.

TradeLens (2019): New members set stage for next wave of TradeLens growth, TradeLens, URL: https://blog.tradelens.com/news/tradelens-ecosystem-update/ (Accessed 2019-10-04).

Vengadasalam, S., Kleinfercher, F., Lawton, J. (2019): Bloxberg – The Trusted Research Infrastructure, Whitepaper 1.0, Max Planck Digital Library (MDPL).

Wood, G. (2014): Ethereum: A Secure Decentralised Generalised Transaction Ledger, URL: https://ethereum.github.io/yellowpaper/paper.pdf (Accessed 2019-10-04).

Woschnak, K. (2005): Rechtsberatung – Mittlerin zwischen virtueller und realer Welt, Festschrift Nikolaus Michalek, Manz, p. 401–413.

Woschnak, K. (2018): Künstliche und emotionale Intelligenz – Gedanken zur Digitalisierung des Rechtslebens, Festschrift Ludwig Bittner, Manz, p.825–839.

Xu X., Weber I., Staples M., Zhu, L., Bosch, J. (2017): A Taxonomy of Blockchain-Based Systems for Architecture Design, in: 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, Gothenburg, Sweden, p. 243–252.