Digital identity on the blockchain: a cautious primer

Yackolley Amoussou-Guenou[1], CRED, Université Paris-Panthéon-Assas

Enka Blanchard, LAMIH, Université Polytechnique Hauts-de-France & Centre Internet et Société, CNRS, enka.blanchard@cnrs.fr

Djohar Sidhoum-Rahal, OMIJ, Université de Limoges

Over the decade since Bitcoin came into public consciousness with its first major bubble, scholars from a large variety of fields investigated this purportedly revolutionary technology and its impacts on society. However, it took some years before major legal efforts were undertaken beyond the academic realm, first in a regulatory approach and more recently when considering the legal and administrative applications of this technology. As some consider using it to handle digital identity, this chapter seeks to give legal scholars some grounding on blockchains, their advantages, use cases, and limits.

To start with an intuitive definition, a blockchain is a distributed database. However, unlike some distributed databases where anyone can modify the content without maintaining a persistent history of modification (e.g., most of Wikipedia), blockchains have a temporal ordering of every modification. More importantly, they also ensure that all information in them respects a form of "validity" which prevents illegitimate edits and comes partially from a form of consensus. In this regard, Bitcoin was neither the first blockchain — that title goes to a notary blockchain published in the New York Times since 1995[2]— nor the first electronic currency — which was invented by David Chaum[3] in 1983. Bitcoin, however, was the first system to combine both ideas to have a widespread impact.

We do not see this as a simple coincidence. Rather, inspired by Pablo Rauzy[4], we understand this as partially stemming from the fact that the tool had found its niche. Indeed, the blockchain can guarantee the validity of the information on it only insofar as the information concerns the blockchain itself. This is true for cryptocurrencies, where writing is performative in the sense that writing "person A owns 10 tokens" and having this information accepted by other actors makes it true. However, any other information — such as real estate ownership data — risks running into an oracle problem, whereby the veracity of the information depends on an external validator that

[1] The authors are indicated in alphabetical order as they contributed in similar proportions.

[2] See Dberhaus, D. (2018). The World'’ Oldest Blockchain Has Been Hiding in the New York Times Since 1995. Vice. https://www.vice.com/en/article/j5nzx4/what-was-the-first-blockchain.

[3] See Chaum, D., (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology: Proceedings of Crypto 82. Boston, MA: Springer US, 1983.*

[4] We recommend this article (in French) for a more in-depth introduction to the blockchain's functioning, intended for non-specialists: Rauzy, P. (2023). "Promesses et (dés)illusions", *Terminal*, https://doi.org/10.4000/terminal.9059. [Online since 15 April 2023], 136..

makes the link between the blockchain and the material world[5]. This would explain the struggle of many blockchain initiatives which were perceived as a “solution in search of a problem”.

Thus, any proposal to use it should be critically analysed, especially when they are meant to augment or partially replace critical infrastructure, such as digital identity. This means not just looking at the necessary conditions that could make such uses legitimate but also keeping in mind the differences between an imagined ideal system and the reality once implemented, which might be comparable to the existing infrastructure. Indeed, any system used in the real world comes with its lot of bugs, inaccuracies, and vulnerabilities as well as ad hoc modifications due to political and legal considerations, all of which can break fundamental aspects[6].

Although we aim to give definitions and general considerations on the question of using blockchains for digital identities, we should warn readers that many of our frameworks and examples are influenced by a civil law tradition, and more specifically a French one. We will also use multiple examples from blockchains not focused on digital identity as they have been more extensively studied.

This chapter is structured as follows. We will first go over general considerations on the blockchain (definitions, assumptions, limits...). We will then analyse the specifics of using blockchains for digital identities and the corresponding constraints. Finally, we will discuss questions of ecological and social responsibility, as well as sociotechnical aspects which impact the large-scale deployment of such tools.

1. General considerations

1.1 Blockchain fundamentals

As briefly introduced, a blockchain is a distributed ledger, i.e., a list of records on which no-one has full control, and where technically, everyone can participate in building it. In short, a ledger with no central authority. Due to the distributed nature of such systems, and to reduce overhead, transactions are not stored individually but in batches called blocks. A blockchain is structured as a chain of blocks (hence its name) where each block refers to the previous block[7] in the chain (by using the identifier of the block). Therefore, given any block in the blockchain, by following the links to parents, thanks to the identifiers, one must reach the first block in the blockchain. The identifier of a block is the *hash* of that block, which is the result of a mathematical function taking the entire data as input and producing a string of characters as output. This string or *hash* can serve as a signature as it is not computationally feasible[8] to create a different block of data with the same exact *hash*.

[5] This problem happens in any context featuring trusted third-parties, including service “identities”, (e.g., the link between IP and DNS is generally outsourced to a trusted DNS provider — often the user's internet access provider).

[6] See Debant, A., & Hirschi, L., (2023). Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. In *Real World Crypto Symposium.*

[7] Technically, all blocks in a blockchain except one refer to their parent block in the chain. The only block that has no parent is the first block (called *genesis* block) which sets up the blockchain.

[8] This is true for existing machines and only insofar as the mathematical function used is well-chosen and correctly implemented.

Thanks to this chain structure, modifying the blockchain is close to impossible. In fact, changing the content of a block changes its identifier, and the subsequent block does not have a valid reference anymore. Moreover, since the blockchain is a distributed system, many actors store the blockchain on their own devices. If one actor tries to alter the historical data on their local copy, other actors can discover the alteration and reject the change when that user tried to spread it. The definition and design of the blockchain suggests that modifying the already included blocks are impossible. That explains why some says that a blockchain is tamper-resistant[9]. Therefore, the way to make a blockchain evolve is to add new information (in the form of blocks) in an append-only manner, i.e., only at the end.

The information appended at the end in a blockchain can be of two types. Either simple transactions or smart contracts transactions. We call "simple transaction" transactions where one actor sends an asset (usually an amount of cryptocurrency) to another actor; we can see those transactions as a transfer of assets. Smart contracts, on the other hand, are applications written on chains that are executed under specific conditions defined in the blockchain and inside the smart contract. For example, "The 1 Bitcoin at this address that belonged to A now belongs to B" is a simple transaction, whereas "Whenever A will receive 1 Bitcoin from B at this address, 0.5 Bitcoins will be taken from it and sent to C" is a smart contract (albeit a very simple one). Smart contract information on the chain could be "the creation of the smart contract", writing it to the chain, the "call of the smart contract", which is when an actor is using the smart contract with a given input… All information used by a smart contract needs to be written on the blockchain. Thanks to that, all actors in the blockchain get the exact same answer when executing the smart contract (in their local blockchain). As for any other information on the blockchain, no one can lie about the execution of the smart contract (although that does not mean there are no risks, as detailed below).

Some factors (like the absence of central entities, the anonymity, the network, etc.) force the actors building the blockchain to work by establishing a repeated sequence of consensus. In particular, blocks must respect certain validity constraints: which types of transactions feature in the data, how a transaction can be considered valid, how to avoid double spending[10], etc. actors who add new blocks must verify everything to avoid including invalid transactions and, therefore, invalid blocks. In some way, the actors agree to "follow" a protocol defining the rules of the consensus, and how to reach it. Each blockchain has its own consensus protocol, for example, Bitcoin[11] uses a concept known as proof-of-work. It consists in showing how much energy[12] an actor is willing to spend on the blockchain by requiring the expense of a massive amount of computing power. This amount

[9] See Austin, T.H., Di Troia, F., (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In: Bathen, L., Saldamli, G., Sun, X., Austin, T.H., Nelson, A.J. (eds) Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science, vol 1683. Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6.Austin et al., 2022 ; and Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology [online], https://doi.org/10.6028/NIST.IR.8202

[10] Double spending in blockchain refers to the situation where an actor uses the same money twice. For example, if actor A has 1 amount of a cryptocurrency, they should not be able to send that token to two different actors. More generally, it can be seen as using more than the money we have and can spend.

[11] See Nakamoto, S., (2008). Bitcoin: A peer-to-peer electronic cash system [Online] URL : https :// bitcoin.org/bitcoin.pdf

scales in a way to prevent any single actor from obtaining too much control over the blockchain. This computing work, which cannot be useful for anything else, is what makes the proof-of-work in large blockchain a non-negligible environmental harm. That concept[13] inspired the majority of publicly known blockchains until late 2022. The other famous (and, since September 2022, the main) protocol is called proof-of-stake, used by Ethereum among others[14]. In proof-of-stake, instead of spending energy, actors stake some of the cryptocurrency they have in the chain. This protocol is less energy-intensive than proof-of-work protocols, but creates concerns over whether or not it is more centralised[15]. Many other protocols exist but are less known (e.g., proof-of-authority, proof-of-elapsed time, proof-of-reputation, etc.). As the rules are written in the first block of each blockchain, and can only be updated or amended in future blocks, anyone reading the whole blockchain knows all its rules without uncertainty. All blockchain protocols function by checking the validity and then spreading an actor's proposed block. If a high proportion of actors comes to agreement on a certain block, it will eventually be accepted by all others who will include this block at the same place in their local copy of the blockchain.

One limitation of the blockchain comes from the fact that all operations are recorded in the ledger, making it grow with time, taking more and more space. This growth is at least linear but can be faster if the block size is variable. To address this, one solution often used is to make snapshots, which describe the full state of the blockchain at a given time. This reduced state can be compressed and much more space-efficient but still allows the checking of any block added afterwards. However, it removes the ability to individually check the authenticity of transactions before the snapshot (and hence of the snapshot itself). It remains necessary to maintain the full ledger on some servers to be able to perform full audits going back to the beginning of the blockchain. One can liken this to the practice in multiple legal systems where legislators regularly vote on new legislation consisting of modifications (or amendments) to existing laws. Instead of manually compiling the list of modifications, most legal scholars and practitioners tend to follow *consolidated*

[12] Energy here can be understood in two ways. First the work the actor puts into making the chain grow, and second, the energy consumption needed to do the massive computations. Both senses are valid here.

[13] In Bitcoin, when two actors trying to extend the chain succeed simultaneously, there is an inconsistent situation where different actors may have different local chains. actors keep and continue working on the chain with the most blocks to correct such an inconsistent situation in the long run. That is called the longest chain rule in Bitcoin. The combination of the proof-of-work and the longest chain rule forms Bitcoin's consensus protocol.

[14] See Buterin, V., Hernandez, D., Kamphefner, T., Pham, K., Qiao, Z., Ryan, D., Sin, J., Wang, Y., & Zhang, Y. X., (2020). Combining GHOST and casper. *arXiv preprint* available at https://arxiv.org/abs/2003.03052

[15] See Dong, L. B. T. T., (2022). On the limiting distribution of shares in Proof-of-Stake. *Available at SSRN.* URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217095 ;

and Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., & Wang, G., (2019). Compounding of wealth in proof-of-stake cryptocurrencies. In *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23* (pp. 42-61). Springer International Publishing;

and Roşu, I., & Saleh, F., (2021). Evolution of shares in a proof-of-stake cryptocurrency. *Management Science*, *67*(2), 661-672.

texts (such as those edited by Dalloz, Larcier, LexisNexis, LegiFrance). These are easier to handle, although they introduce the risk of errors as raised by the work of Luc Pellissier[16].

1.2 De-centralisation

In the most general sense, saying that a blockchain is decentralised means that there is no central entity controlling the blockchain. However, there are different way of being decentralised. The first example of blockchain we gave in the introduction is the one historically featured in the New York Times. It is a centralised ledger, since any addition to it is totally under the control of the New York Time's editorial board. However, the validity of all blocks can be checked by someone with access to (authentic) archives of the newspaper.

Another example is the now (in)famous and abandoned Facebook Libra / Diem project. While that blockchain may seem centralised, it was not but was meant to be controlled by a consortium of entity gathered as the Diem Association. All members of the consortium were able to construct and add blocks to the blockchain by means of consensus, while every user of the blockchain, while not able to build/add blocks, could propose transactions. Such blockchains where the right of write (adding blocks/participating to the consensus) is managed by a predefined set of actors are called consortium blockchains. An analogy can then be made with an oligarchy, as a reduced set of actors hold specific powers over the whole system (sometimes but not always including the power to induct others into this reduced set).

Both examples given so far are what are called public blockchains since anyone can read the transactions written in the blockchain. There is no need to have a specific access. Bitcoin or Ethereum are public blockchains that are more "open" in the sense that anyone can enter without permission in the blockchain and emit transactions without going through an identification process[17]. In Bitcoin or Ethereum, users do not have to go through that, moreover, if they follow the consensus protocol (proof-of-work in Bitcoin or proof-of-stake in Ethereum), they are also participating in adding blocks, therefore, anyone also has the right to write (in the sense that they can actively take part in the consensus).

Some other blockchains need the different actors to be identified, but then all registered actors have all the rights. These blockchains are private blockchains. Aside from requiring permission when new actors seek to enter the system, they can be built the same way as public blockchains. Since we defined the blockchain as being distributed (and therefore decentralised), all the examples mentioned, except the one from the New York Times, can be qualified as blockchains.

Lastly, we would like to mention that decentralisation is not a question of geography but one of power and interests. If a blockchain is controlled by a single actor, even if that actor has geo-distributed servers (i.e., severs present in multiple geographic area), it does not count as decentralised, and we should not call it a blockchain.

[16] LSee.Pellissier, L. (2023). Versioning the law. Rencontres d'hiver du GT SCALP https://www.irif.fr/gt-scalp/journees-2022.

[17] In the Diem project, it was planned that users of the blockchain, those emitting transaction must have an account on Facebook or on other Meta platforms.

1.3 Necessary conditions

One cannot analyse the security of a blockchain without expliciting the setting and underlying assumptions. As such, nearly all blockchains make use of some common assumptions, which we'll explain here (although not all would be relevant for a blockchain handling digital identity, they should still be kept in mind).

The first one is that they assume that current mainstream cryptography is secure — a reasonable assumption, which nonetheless still needs to be explicited. This comes into play in two places. First, the proof-of-work mechanism generally depends on the existence of mathematical functions (hash functions) that are used to create hard challenges. That is, it is hard to compute the solution to the challenge, but easy to check that the answer is correct. The same kind of function is also used to guarantee the authenticity of each block by making sure that one cannot replace a previous block by a forgery as it makes it computationally unfeasible to compute a forgery with the same identifier. If the functions currently used were in fact vulnerable, it would open blockchains to many kinds of attacks. However, three factors make it unlikely that this vulnerability already exists. First, it would have much more dire consequences as it would also open attacks on the entire internet infrastructure and allow decryption of almost all secure communications. Second, an already massive amount of effort has been made to attack such functions by researchers from all over the world (often with a vested interest in making any result public), making it less likely that a small group would succeed where many have failed. Third, some other functions have been studied and found wanting, including one proposed by the NSA with a hidden weakness that would have allowed it to be decrypted (only by the NSA), indicating that even powerful actor's attempted attacks can be discovered (Hales, 2013)[19]. Finally, even if one key cryptographic component was found to be vulnerable, many blockchains integrate an ability to update which mathematical function they use, and it might lead to only a temporary crisis[20].

The second assumption, which is more often made explicit, is that no group of users should be able to take even temporary control of the blockchain, such as by having a majority of the computing power (for proof-of-work) or a majority of the assets (for proof-of-stake). For example, if a consortium held more than 50% of computing power on Bitcoin, it could decide which transactions are accepted and could engage in double spending, although it would still not be able to steal assets. This is supposedly prevented for Bitcoin by the sheer scale of the computing power required but smaller blockchains are vulnerable. Moreover, as smart contracts allow a wider range of operations, they also allow for more complex attacks, including ones that can steal assets. For example, the *Beanstalk Farms* blockchain was attacked in April 2022 by attackers who temporarily borrowed enough to acquire a controlling stake, voted through the internal mechanism to give themselves all the blockchain's existing assets, and sold everything back, netting them 182 million dollars in less

[18] On this point, see the contribution on authentication and authorization in the present book.

[19] Tee.Hales, T.C. (2013). The NSA back door to NIST. *Notices of the AMS*, 2013, 61, 190-192.

[20] In the case of cryptocurrencies, the crises have been resolved by reaching a consensual decision to change the rules. This can be partially explained by the fact that a found vulnerability could lead to a crisis of trust and hence to a fall in asset value, giving a strong incentive to reach this decision.

than 13 seconds[21]. This was made possible by existing decentralised finance[22] toolsets, allowing instant loans and immense leverage despite limited collateral. Although such attacks are mostly doable on small and medium-sized targets (up to billions of dollars, two orders of magnitude below Bitcoin and Ethereum), it bears repeating that the vast majority of crypto-assets are held by a minority (with more than 20% of even major blockchains sometimes being held by a single individual[23]. Finally, blockchain protocols are meant to resist the presence of some malicious actors (by preventing a small minority from taking control), but those very protocols can make it harder to prevent or repair individual harms than in a system with a centralised authority. For example, it is generally not feasible to distinguish a small group pretending to be victims of some fraud from a group of malicious actors. The absence of a centralised authority means that both users who make mistakes (e.g., by losing their password or device) and those who fall victim to scammers do not generally have any recourse[24].

The third assumption is that the systems are implemented correctly and do what they purport to do, and that the systems will not need to evolve in any unplanned way. The central feature of smart contracts, blockchains and more general computerised systems is also one of their main drawbacks: they do exactly what they are coded to do. If a flaw is found in a piece of code[25], nearly nothing prevents its exploitation, as happened on Ethereum with the famous attack on The DAO[26]. There are generally no ways to cancel previous operations or delete data on most blockchains, except by convincing users to accept fundamental changes in the structure of the chain, which generally creates a *fork* (that is, a situation where two groups of actors have different and inconsistent local chains without reaching consensus, leading to two distinct chains). Moreover, the longer one waits before acting, the more it can impact the rest of the chain. When considering a blockchain for digital identity, this raises critical questions. For example, if a mistake is found in someone's

[21] Jee.Benson, J. (2022). Ethereum DeFi Protocol Beanstalk Hacked for $182 Million—What You Need to Know [.nline] URL: https://decrypt.co/98118/ethereum-defi-protocol-beanstalk-hacked-182-million-what-you-need-know;

[22] Following Wikipedia's definition, decentralised finance offers financial instruments without relying on intermediaries such as brokerages, exchanges, or banks (as of 11-06-2023).

[23] ASee Sai, A.R., .uckley, J., and&Le Gear, A. (2021). Characterizing wealth inequality in cryptocurrencies. *Frontiers in Blockchain,* 4, 730122.

[24] This is sadly not a small population, as it is estimated that close to 20% of bitcoins are lost and unrecoverable. See:https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html.

[25] Article 30 of the European Data Act tries to address this by mandating a high robustness for all smart contract (although its focus as of version COM/2022/68-final limits its range of application). However, considering that guaranteeing such robustness was at the heart of many smart contract initiatives which still became hacked, one can wonder whether this will have a noticeable impact.

[26] Mee Mehar, M., Chier, C., Giambattista, A. Gong, E. Fletcher,G., anayhie, R., Kim, H.M., and askowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. *Journal of Cases on Information Technology (JCIT)*, 21(1), 19-32;.

and Sayeed, S., Marco-Gisbert, J., and Caira, T. (2020). Smart contract: Attacks and protections. *IEEE Access*, 8, 24416-24427.

filiation today, the state can resolve the issue by making a limited set of corrections, most of it on documents belonging to that person and their descendants. If a mistake was found on an identity blockchain that had not planned a procedure to address it, correcting it could potentially invalidate any and every operation saved on the blockchain after the initial mistake. However, no system can reasonably plan for all eventualities in advance, especially one tied to concepts as sensitive and culturally-dependent as identity. For an example of potential conundrum, allowing for the possibility to change a gender marker on a digital identity blockchain seems reasonable. However, it is not evident in advance how to handle this in details as legislations are currently evolving on the recognition of intersex rights. In certain jurisdiction, it is illegal today to allow for (even the theoretical possibility of) more than two genders, while legislators and courts could agree in the future that the state has a responsibility to respect more complex gender and sex identities. Moreover, as the data on the blockchain is not meant to be erasable, this could come into conflict with the right to amend one's data (especially within the framework of GDPR), depending on where said data is used.

1.4 Tool adequacy

Given the aforementioned information, for a blockchain to be interesting to use, or even simply for its use to be justifiable, actors that can “write” in the blockchain (those taking part in the consensus) should not be managed by a single entity. In short, there should be decentralisation of those actors. If one does not require decentralisation, a centralised ledger, managed by the corresponding entity, would generally be sufficient and more efficient.

The need for transparency can also explains the use of a distributed ledger (and blockchains for example). But that requirement enough should not be sufficient, as there are systems allowing to have some sort of transparency without the machinery of blockchains, such as public bulletin boards (which have cryptographic equivalent guaranteeing good properties such as transparency, see Heather and Lundin, 2008[27]).

Another interesting point to mention, linked to the previous one is that one may be interested in using a blockchain if there is a lack of trust. Since blockchains theoretically operate in a decentralised manner and with transparency, there is no need to trust any given actor. As often said in the blockchain community, “(do not) trust, but verify”. Such requirement is important for considering a blockchain as an interesting platform to use, but does not seem a mandatory one. In some sense, actors trust the (consensus) protocol of the blockchain to guarantee the properties they aim to have, often without other proof of their correctness. In practice, the popularity of service providers such as cryptocurrency exchanges (e.g., Binance or Coinbase) shows that some users choose to trust third parties and that the system is not as decentralised as many think. Moreover, the question of trust is much more complex to handle with smart-contracts (in part because it regularly happens that major vulnerabilities get found in some contracts).

[27] Jee Heather, J., and&Dundin, D., (2009). The append-only web bulletin board. In *Formal Aspects in Security and Trust: 5th International Workshop, FAST 2008* Malaga, Spain, October 9-10, 2008 Revised Selected Papers 5 (pp. 242-256). Springer Berlin Heidelberg.

2. Potential uses of digital identity blockchains

Before considering how (and whether) to implement digital identities — and thus the usefulness of blockchains for such purpose — a first question is to decide whether one expects a 1-to-1 matching between digital and physical identities, or if someone can have multiple digital identities. This is especially relevant when one considers what a digital identity (DI) is supposed to accomplish. We see two main potential objectives in that regard, which are often tied. First, the DI could be used to allow the individual to access services, interact with others, and exert their rights. In many cases (e.g., signing contracts or voting), the latter could require the unicity[28] of the DI. Second, the DI could be used by institutions (and private actors) to regulate their interactions (and potentially keep track of them). In such a case, forcing a 1-to-1 matching reinforces the surveillance apparatus (whether it is for policing, for targeted ads or any other reason), although even allowing multiple DI would not necessarily be a solution (e.g., if some actors can link the different DI). The following will assume this equivalence between physical and digital identities as this framework is both common and simple, although requiring this equivalence is a political and design choice and not a necessity.

Once this question is solved (which depends on contexts and stakeholders[29]), a second question arises if one wants to use a blockchain: what kind of blockchain? Beyond technological considerations, this also means deciding which actors can act and interact on it, and the kind of power they have. Starting from the assumption that the blockchain is not fully centralized — and thus is a legitimate blockchain — one needs to take into consideration the underlying legal and administrative systems. For example, the French legal and administrative tradition follow a very centralised conception of identity[30], which would naturally influence any digital identity used in such a legal system. Unlike many common law systems where it is possible to change fundamental aspects of one's identity by simple declaration (as in the United Kingdom), any modification (even to a first name) needed to go through a judiciary process until 2016 (when article 60 of the French Code Civil was amended to simplify the process by requiring administrative but not judiciary approval[31]). It would then stand to reason that states following a civil law tradition would avoid relinquishing such powers from the state's monopoly. As decentralisation generally transforms the power relationships to accommodate more actors' interests, one would expect some reluctance to

[28] In some cases such as voting, unicity of the digital identity is not technically necessary as long as there is a mechanism preventing a person from voting as multiple identities, or taking this into account if voting more than once is allowed, s was historically the case for citizens with land holdings in multiple constituencies in the UK. S,e S Shaw-Lefevre, G. (1892). "Plural Voting (Abolition) Bill (No 42)". *Parliamentary Debates (Hansard)*. United Kingdom: House Of Commons. Col. 1184.

[29] The stakeholders could for example involve the population, the decision-makers, and different administrations.

[30] While there is no legal obligation for a French citizen to get an ID card from the state, many aspects of the French administration are made tremendously difficult without one to nudge people to possess such a document.

[31] Despite this increase in one's agency (which recently expanded to certain cases of last name changes), there is still a gap between legal texts and their practical application (see Décision-cadre du Défenseur des droits n°2020-136).

develop a national identity blockchain in which the state does not have sufficient technical privilege to maintain its sovereignty over such affairs[32].

One of the most constrained ways to use a blockchain for digital identity would then be as a tool between state administrations, as those are sometimes legally prevented from sharing databases. One could then imagine a system where some central aspects of identity (including full vital records) exist on this blockchain, with only specific state actors being allowed to change the information. This could be set up in a way to help users[33] by providing a singular interface and the ability to easily provide certified or authenticated documents which would belong natively on the blockchain. It could also simplify existing logistical issues[34] when changing some aspects of identity (such as one's marital status, name or gender). This could also help maintain a continuity of identity despite allowing some incremental changes.

This brings us to a fundamental distinction between errors and changes, which would need to be addressed. A change or rather an update to one's identity (e.g., a name change following a marriage) does not create ambiguities regarding whatever happened before the update. This is distinct from an error needing to be corrected, such as a spelling mistake on the original birth certificate that gets discovered decades later. This situation could affect all the individual's documents whose validity on the blockchain cryptographically depends on the validity of the original documents. Thus, although one's agency might be reinforced when it comes to voluntary changes of identity, a centralized authentication system might have more agility than a distributed one when it comes to correcting mistakes. Error handling is an issue for which solutions should be planned for in the early phases of design.

We can now build on the previous idea of a central blockchain for identity by remembering that each blockchain is, fundamentally, a distributed database. One could then extend some writing rights not just to state administrations but to a larger set of actors: universities, medical practitioners, notaries... The blockchain could then serve, as a common repository (albeit decentralised) for people's various official documents (e.g., diplomas or medical prescriptions), whose authenticity would be easier to check. One important consideration is that, whether in this context or the ones below, this personal data would have to be encrypted, and decryptable at will but only through the user's intervention (or potentially certain authorities). Some universities have already started putting diplomas on blockchains but as these are not directly tied to any solid digital identity, they rarely address the problems that they are trying to solve — independently of the importance of said problems[35]. France also has a recent project to deploy a consortium blockchain

[32] See Coutor, S., Hennebert, C., & Faher, M., (2020). Restitution des ateliers du groupe de travail « blockchain et identité » (BCID), *Rapport d'étude du Ministère de l'Intérieur*.

[33] We use the word users as they would not strictly correspond to either the set of citizens or the set of inhabitants.

[34] The authors have personally observed that existing French databases do not automatically update this kind of information (even for the ones sharing a common access through FranceConnect, the French administrations' online authentication system for users). One mechanism exists to make a general change, by making a demand to INSEE to make a correction and transfer it to all other state actors. However, this is only available to French citizens born in metropolitan France or some overseas territories.

[35] Rauzy's previously mentioned article also discusses using blockchains for diplomas.

recording notarial information[36] and especially real estate transactions, whose accuracy would be guaranteed by the contributing notary's legal obligations (as actors already empowered by the state to do so), although some have criticised this project as misunderstanding some fundamental aspects of trusts within blockchains[37]. In this new kind of configuration with a digital identity blockchain, the state itself would serve as a guarantor and oracle to ensure the link between the blockchain and the material realities.

Although increasing the set of actors who can contribute to it can greatly extend the usefulness of the blockchain, it also comes with its risks as there would be more opportunities for errors. The existing systems already can fail in non negligible ways, with for example the case where the courts decided that Akim Oualhaci, a French civil servant had been a victim of discrimination in a national competitive examination, leading to the retroactive cancellation of that examination's results[38]. This left the selected candidates in a temporary legal and employment limbo, despite there being human decision-makers at every step of the process who could try to limit the collateral damage. In a blockchain where such administrative procedures would be certified, a retroactive reversal of such decisions could have wide-reaching influence. To take a different potential example, if a doctor was found to have cheated their way into their diploma, their patients' prescriptions might suddenly become invalid. This kind of issue would be compounded if one allows privileged actors to create new privileged actors. This is where the canon law concepts of *liceity* and *validity* could come into play, whereby one could deem an initial action[39] to have been illegitimate (illicit) without cancelling its outcomes (and their respective consequences). In all cases, the design should ensure that any cancellation of an actor's action should have bounded consequences, at most, by that actor's reach and not affect people arbitrarily far from the error.

In all the cases above, the actors allowed to modify the blockchain — or even just to propose modifications — get this power in some way from the state, which thus keeps a form of control over the blockchain's information (and its evolution) but mostly has a complete control over the *kind* of information allowed on the blockchain. However, one could also envision a more open blockchain where the digital identity part — still guaranteed by the state — would be used as a basis and a building block for a more diverse ecosystem of applications (as is the plan for the current France Identité project[40]). This would allow other actors to contribute new tools (using smart

[36] See Notaires de France (2021). Le numérique, l'homme et le droit. Accompagner et sécuriser la révolution digitale. *Rapport du 117e congrès des notaires de France.*

[37] Cee Chaserant, C., Dauchez, C., Sarnay, S. (2021). Du notaire à la blockchain notariale : les tribulations d'un tiers de confiance entre confiance interindividuelle, confiance institutionnelle et méfiance généralisée, *Revue juridique de la Sorbonne*, n° 3.

[38] ee https://www.radiofrance.fr/franceculture/gloire-jeunesse-et-gros-reseau-le-recrutement-au-cnrs-est-il-arbitraire-1031980

[39] This kind of case made the news a few times in recent decades with variable outcomes when multiple archbishops (chiefly Lefebvre and Milingo) were found to have illicitly ordained others and were excommunicated, questioning but not automatically refuting the validity of the ordinations themselves. See Zagano, P. (2011). Women & Catholicism. Gender, Communion, and Authority. Palgrave Macmillan.

[40] See Karamanli, M., Hennion, C., and Mis, J.M. (2020). Rapport d'informationpar la mission d'informatique commune sur l'identité numérique. *Assemblée Nationale*

contracts) and allows a wider range of possibilities, such as signing contracts on material assets (with the state potentially still serving as an oracle).

All the possibilities above consider uses of a blockchain that do not require changes to our current political or socio-economic systems. However, we want to mention one more potential use that does require fundamental differences. Just like Drakon provided the first written constitution for the Athenians, giving everyone — who knew how to read — the ability to know the laws, a blockchain could be used to publicly handle legislation in a system of direct democracy. There are many variants depending on whether any actor has a privileged status, on how to propose laws and vote on them, but nearly all of them require a solid grounding on identity to ensure equal voting rights.

3. Concluding remarks: digital identity blockchains in their social contexts

We have discussed an array of potential use cases for digital identity blockchains — with no claim to exhaustivity — as well as some of the main considerations to keep in mind when designing, deploying or using them. However, the above does not give a full picture as we have considered systems that function normally or that have to handle errors, but no adversarial component. Indeed, beyond changes in identity and errors, fraud, (involuntary) identity sharing, theft and non-compliance are critical concerns that would also need to be addressed. Let's for example suppose that a person not only loses their access to their digital identity — which is not a risk that can be fully eliminated — but that said identity (or the means of accessing it) is the subject of a theft or copy. What remedy could exist? Would all the person's documents need to be remade on the blockchain and recertified? What if some of the certifying authorities (e.g., universities) do not exist anymore, or not as the same legal entity? All the above already exist and are detrimental to users (and administrations), and switching to blockchain could exacerbate this harm. This is concerning before even thinking about not just errors but intentional wrongdoing by privileged actors.

Despite these risks, we have mentioned some potentially legitimate uses of digital identity blockchains. They are *potentially* legitimate in that, if satisfying answers were given to all the considerations mentioned above (although not intended as an exhaustive list), one could consider using them. However, that does not directly imply that they would necessarily be the optimal choice as other technologies could be more appropriate. Beyond the limitations we've discussed, there are many other more practical considerations. First, the technology might not be as efficient as other distributed databases for many metrics: bandwidth, operations handled per minute, delay before an operation is confirmed, cost per operation, overhead... Avoiding contributing to existing environmental disasters would also presumably mean avoiding any large-scale system based on proof-of-work[42], note that using proof-of-stake does not guarantee being good for the environment since multiple existing systems based on proof-of-stake have huge environmental impact[43]. Second, its widespread use could create unforeseen issues due to how people will change their habits to

[41] See the contribution on authentication and authorization in the present book.

[42] Aee chapter 2.5 of A. Auvolat, (2021). Probabilistic Methods for Collaboration Systems in Large-scale Trustless Networks. PhD Thesis defended at Université de Rennes 1.
See also U. Gallersdörfer, L. Klaaßen, C. Stoll, (2022). Energy Efficiency and Carbon Footprint of Proof of Stake Blockchain Protocols. CCRI Report.
See also A. De Vries, (2023) Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. *Patterns,* 4 (1).

respond to the technology (potentially by trying to fight it), even as some issues mentioned above still lack good answers.

There are multiple available examples affecting the legal side, which are not restricted to blockchain technologies. First, and although they are not absolutely necessary to implement digital identity on a blockchain, smart contracts still suffer from some unclear regulations, especially on who is responsible when one contract is found to be vulnerable[44]. The existing and proposed legislation (such as the EU Data Act[45]), only covers some cases, with a focus on smart contract vendors. This leaves a grey zone for those who develop them as public service (as with open-source software), as well as jurisdictional issues. A second issue affects the individual rights of the people who could be pushed to adopt digital identities despite their own preferences. One might imagine a "right not to be digitalised", but even if that right were guaranteed, one should not underestimate the extent to which states could "nudge" their population into adopting these systems by maintaining alternatives with degraded service[46]. For example, in France, since the digitalisation of income tax return, although it is still possible (under some circumstances) to make a paper form declaration, delays are clearly shorter in the latter[47]; the same applies when one wants to get a driving license where not using the digital services implies using lengthy processes. Third, some technologies (such as e-voting, secure messaging, online authentication) suffer from a poor understandability which affects not only the general population but also sometimes judges, which can give rise to non-sensical decisions on technological issues. This is compounded by the fact that many of the existing documentation on blockchain technologies come from people with vested interests in increasing its use, to the point that academic research also sometimes falls for scams and integrates biased or unverifiable results[48].

[43] Uee .allersdörfer, U. Klaaßen, L., Ctoll, C. (2022). Energy Efficiency and Carbon Footprint of Proof of Stake Blockchain Protocols. *CCRI Report*.

[44] This does not even address the question of whether some existing "hacks" like the one which affected Beanstalk Farms could in fact just be termed a form of arbitrage, as their structure is very similar to a leveraged buyout.

[45] Adopted in July 2023, the EU Data Act will apply 20 months after its publication in the Official Journal of the European Union, so from early to mid- 2025.

[46] A long-term concern is also that, unlike paper records (when well kept), any digital system meant for storage requires constant maintenance (both in hardware and software) or risks becoming inoperable in a matter of decades if not years.

[47] https://www.service-public.fr/particuliers/vosdroits/F358?lang=en

[48] See Elanchard, E. Li Vigni, F., and Rauzy, P. (2022) Auteur·ices, relecteur·ices : redoublons de prudence face aux effets de modes technologiques. [online]⟨ *Available at https://hal.science/hal-03741811*

Many states and suprastate actors have engaged in the study of the different uses of blockchains, from currencies to digital identities. Although there is a legitimate interest in this study, one should not underestimate how much of it is driven not by a need for improved solutions but by hype or lobbying for products that are often worse (ecologically, economically, security-wise, etc.) than existing alternatives. Moreover, there is a wide gap between investigating the benefits (and drawbacks) of such technologies and deploying them at large scales without a full civil debate with all stakeholders, especially the population. The first stage — seeing what is possible and what isn't — is well underway. However, we should not forget a second stage: going back to see whether the proposed solutions do address the issues, and are better than the alternatives, not only in an idealised world, but when faced with the frictions of reality.

[49] See for the report on blockchain for identification on behalf of the French Ministery of Interior : https://www.interieur.gouv.fr/actualites/actualites-du-ministere/technologie-blockchain-revolution-pour-lidentification.
See also, for elements of the European commission's blockchain strategy :
- https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure
- https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy