ARTICLE:

Berlin to Dublin to Beijing: Blockchain's trail

By **Ugo Bechini**

Circa 1748, near Berlin. When Frederick[1] was building Sans Souci Castle, an existing mill hindered his plans; the king asked the miller to decide himself the price for the mill. The miller replied that his family had owned the mill for a long time, father to son, and he did not want to sell it. The king became more pressing; he even offered, in addition to the price, to pay for the building of another, better located mill. The stubborn miller insisted he wanted to preserve what he had received from his ancestors. The king, furious, summoned him and said, with an angry voice: *Why do you refuse to sell your mill, despite all the advantages I offer you?* The miller stayed the course, and the king continued: *Do you know I can take the mill from you without any payment? Yes,* the miller replied*, if it wasn't for that court sitting in Berlin*.[2]

Two hundred and fifty years later, near Dublin. On 4 September 1998, the President of the United States of America, Bill Clinton, and Irish premier (Taoiseach, to be precise) Bertie Ahern, for the first time in history,[3] digitally signed an international treaty using the products of a local software house, Baltimore Technologies from Dublin. The event did not prove auspicious. The Gateway plant that hosted the ceremony closed in August 2001 due to lack of orders.[4] Baltimore Technologies, which in 1999 was still the world leader in the field, with a capitalization of 13 billion US dollars, closed its activities in December 2003.[5] The historical 1998 ceremony, to be honest, had a curious epilogue, which in hindsight could be said to be revealing. Signatures made, the two leaders stood and purposefully exchanged their smart cards.[6] Despite the briefings they had possibly received from NSA, the two men seemed not to have any idea of what they were handling, and therefore exchanged their cards as paper protocols. It became especially evident that the digital signature the two leaders had just performed was entirely useless, even as a liturgical element.[7] In the following years, in fact, the question *what is the digital signature for?* became more and more an exacting one.

Presently, near Beijing and anywhere else in China …

Blockchain: the technology

I will not elaborate on Blockchain's technical layout. I am ready to admit (and I have been for several years now![8]) that such technology is able to keep, in a quite

[1] Frederick II Hohenzollern (1712-1786), known as Frederick the Great.

[2] My translation from *Vie de Frédéric II, Roi de Prusse*, anonymously published at Strasbourg in 1787, a year after Frederick's death; it is generally considered the first printed work that includes this anecdote, later to become famous. I have cut the vaguely hagiographic final lines, that I find somehow contradictory with the rest: *The King felt very flattered by this answer, understanding that he was not believed to be able of committing an injustice; he left the miller in peace, and changed the plan of his gardens*. The mill that is visible today in Potsdam, a few steps from Sans Souci, is a replica of the original building.

[3] As far as I know, the last too.

[4] Jamie Smyth, '900 jobs lost at Gateway as company closes Dublin base', *The Irish Times*, 9 August 2001.

[5] *Baltimore Technologies,* Wikipedia entry, viewed on 1 January 2019.

[6] At 2'38" of the video available online at youtu.be/4ddUdEQjrOo.

[7] Stephen Mason, in the third edition of *Electronic Signatures in Law* (Cambridge University Press, 2012), p. 160, fn 55, pointed out that the President of the United States of America, Mr Bill Clinton, signed the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7003 in 2000 electronically using the private key of a digital signature on 30 June 2000. The private key was stored on a smart card. Article 1, Section 7, entitled 'Revenue Bills, Legislative Process, Presidential Veto' of the United States Constitution states that 'Every Bill which shall have passed the House of Representatives and the Senate, shall, before it become a Law, be presented to the President of the United States; If he approve he shall sign it'. Mason went on: 'If a law was necessary (which it was not, because electronic signatures had long been accepted by the judiciary in the USA) to permit the use of electronic signatures, then it was necessary to enact an enabling law to authorize the President to sign the law with an electronic signature. If an electronic signature was not necessary, the Electronic Signatures in Global and National Commerce Act is otiose. If it was necessary to enact the law, then the law as it presently stands cannot be constitutionally enacted for want of either the manuscript signature of the President, or prior enabling legislation.' This reference is now omitted from the fourth edition: *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016) http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence .

[8] Six actually, but they may count as eighteen or even fifty-four, depending on your interpretation of a famous statement from Bill Gates. He once told Bill Clinton that the IT world is three time faster than standard business, which in turn is three times faster than Government; the two of them

reliable way, its promises: creating, without any need of centralized authority, a system of ledgers that will record an indelible and unchangeable trace of certain operations (typically: transfers) which may involve Bitcoins or any other object. Blockchain and digital signature are deeply related, as both have their technical roots in asymmetric key cryptography. In the eyes of the average lawyer, and in general of those who have no mathematical preparation, they share[9] another important feature: they both are, at some extent, counterintuitive. It is not easy to establish how somebody may be in control of a ledger, but has no means to meaningfully alter any of its entries; nevertheless that's on any account true, and we have to deal with it.

Pure Blockchains

In this paragraph I will refer to the pure (or open) version of the Blockchain, the one in which access is open to anybody, and the final beneficiaries of the legal positions directly hold the cryptographic keys that allow them to dispose of such legal positions. These positions can be, so to speak, self-representations (this is the case for Bitcoins, which exist within the Blockchain, and nowhere else) or, on the contrary, objects that have their own life outside the cryptographic representation. The latter is, in such cases, no more than a mere token that represents the objects, and can be exchanged in a Blockchain, the same way Bitcoins are. At least two difficulties arise here.

Firstly, if the legal positions at stake are not (in the proposed terminology) self-representations, we must somehow be able to certify that object and token do actually match. One may design a very interesting Blockchain-based architecture that follows a chicken from the broken egg to our table but, at the end of the day, the correspondence between the token and our meal must be guaranteed by some procedure placed outside the Blockchain. Saying that the quality of our food is secured via Blockchain means telling only one half of the story, while concealing the other (more interesting) half. The strength of a chain is equal to the strength of the weakest of its rings. Invincible algorithms are not a meaningful resource if the intersection between real world and cryptography cannot be managed with the same reliability. Those looking forward to using a pure Blockchain in the real estate domain must face additional problems, which I sincerely believe cannot be solved at the present time. Just an example: real estate changes. On one parcel of land, buildings are erected or demolished; flats are divided and merged; cellars become garages. In short, it is not a matter of transferring immutable units like Bitcoins. In the absence of a recognized authority, who can deliver the landlord additional tokens (or change existing tokens) to account for the apartments built on his land?

Secondly: the loss of the cryptographic key corresponding to the legal position entails the loss of the legal position itself, which will stay inaccessible forever. A lost computer or a forgotten password may cause losses in the realm of the millions of pounds,[10] or the forfeiture (so to speak) of any object that has been associated with the token: real estate too, at least in theory. At the end of last century a witty sentence was in use[11] in order to describe such

therefore were, in his opinion, *out of sync by a factor of nine* (Bill Clinton, The Debriefing, in Wired, December 2000, https://www.wired.com/2000/12/clinton-2/). In 2013 Sabrina Chibbaro and myself suggested *that cryptographic technologies like those used in the Bitcoin scheme* could be employed in order to digitally transfer a legal position with no need for a central authority: in *Rivista del Notariato,* a venerable 73 years old Italian law review, at p. 276, at the end of footnote 13. The circumlocution in italics (maybe better: what now sounds as a circumlocution) is easily explained: the word Blockchain was not yet in common use at that time. Just a couple of lines, but they could well be the first reference to Blockchain in Italian law literature.

[9] It is widely acknowledged that asymmetric cryptography was first discovered in the GCHQ, the British General Communication Headquarters. Despite the spectacular military importance of such breakthrough, the novelty of the concept was scary, even for a top level institution like GCHQ, and the idea was shelved. The story is told by Steven Levy in *Crypto: how the code rebels beat the government, saving privacy in the digital age* (Viking, New York, 2001), p. 313.

[10] James Howells, a Welshman, inadvertently threw away, in the summer of 2013, a hard-disk containing the access keys for 7,500 Bitcoins (Alex Hern, 'Missing: hard drive containing bitcoins worth £4m in Newport landfill site', *The Guardian*, 27 November 2013). In the autumn of that year they were worth about 4 million pounds sterling, and were approaching the 100 millions threshold when the media came back to him four year later (Anthony Cuthbertson, 'Man Accidentally Threw Bitcoin Worth $108 million in the Trash, Says there's 'No Point Crying About It'', *Newsweek*, 30 November 2017). The fateful hard-disk should still be somewhere in the Docksway landfill, Newport, Wales. I do not know if Mr Howells found some relief at the end of 2018, when the value of 'his' Bitcoins dropped to some 20 million pounds sterling.

[11] Mentioned for example by Jane Kaufman Winn, 'The Hedgehog And the Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions', in *Administrative Law Review*, Vol. 51, No. 3 (Summer 1999), p. 955.

scenarios: *Grandma picks a bad password and loses her house*. No need to go into further detail in order to show that this does not work: we need something else, an additional infrastructure layer.

But this is not the end of our problems.

It is often maintained that any business carried out on the Blockchain is tracked. Fine, as long as we agree on the exact meaning of the word *tracked*. In a pure Blockchain, like Bitcoin, no one identifies anyone. The track we get can be described as follows: *in a bulletproof and unchangeable*[12] *ledger can be found an indelible trace of the fact that the unknown holder of the private key corresponding to the public key X, has transferred Y Bitcoins (or Y of any other thing) to the unknown holder of the private key corresponding to the public key Z*. If somebody wants to call this a *track*, I will not raise any objection, but this will not even come close to satisfy the basic requirements of any country attempting to prevent money laundering. It should also be noted that the transfer of a given amount of Bitcoin can be performed in a way that does not leave behind any trail, not even the very subdued one just described. The virtual wallet where Bitcoins are stored can be split, creating a wallet that contains the desired amount: handing over the digital key of the new wallet does the trick. Such procedure leaves behind no digital trail whatsoever, the same way a bank does not know if a rechargeable ATM card with its PIN changed hands.[13]

Let us face the main issue. A pure Blockchain is built on an indefinite number of nodes which record the operations performed; they can be found anywhere in the world, and their location is not planned in advance. In the prototypical case, Bitcoin, the nodes at December 2018 were about ten thousand, scattered in a hundred countries around the world, including China. Beijing's position is manifold. Around 2016, China was a leader in mining activities.[14] This issue will not be addressed here, as it is specific to the Bitcoin model and its economic balance, but not an essential component of any Blockchain; it is to be noted anyway that a working business model is required for any viable Blockchain, and this is not obvious in a pure or open Blockchain, that is not based on a covenant among their operators or some piece of regulation. In 2018, the Chinese government halted mining; they seemed worried,[15] not about the energetic and environmental issues (as noted in a previous footnote) but about the deep anonymity of Bitcoin (and of any other pure Blockchain), that may be easily exploited by criminals.

This remark could be elaborated and lead us very far from the discussion, but I do not want to put forward the scaremonger talk of mafia activities, albeit not fictional.[16] Let us get back to the point. We have an indeterminate number of nodes scattered all over the world. Is it conceivable that a judge, any judge, can effectively order the cancellation (or any equivalent operation) of an operation on Blockchain, performed (for example) under armed threat? Of course not.[17] Moreover, users are anonymous and therefore unlikely to be summoned in court in any other form. We just have to say, recalling the prologue, that a pure Blockchain knows no judge: neither in Berlin, nor in Beijing. That judge who protects (or does her best to protect) consumers, weak and helpless members of society and, if required, even millers. That judge who guarantees (or does his best to guarantee) the rule of law, one of the foundations of Western civilization. A pure Blockchain dwells in a space devoid of law.

This should not even be regarded as a criticism: actually it is a remark many fans of the Blockchain take pride in noting. Significant numbers of articles may be found on the web sporting triumphant titles, such as *Why the Government Can not Kill Bitcoin*, or *Bitcoin is beyond government control*, or even *The*

[12] No pun intended.
[13] I owe this and other remarks to my fellow notary Michele Manente.
[14] Bitcoins have not been issued all at one time: a part of them has been reserved for subsequent acquisitions; anyone can try them through *mining*, which consists in solving mathematical problems of increasing complexity. Only computer systems of monstrous power can now solve them in an industrially profitable way, but their power consumption is on par with the whole of Ireland (Alex Hern, 'Bitcoin mining consumes more electricity a year than Ireland', *The Guardian*, 27 November 2017). This led miners to settle where energy is less expensive, and especially in China, where unfortunately electricity is very often obtained from coal, with the environmental consequences we all know: Anthony Cuthbertson, 'Could Norwegian fjords and waterfalls stop bitcoin from destroying the planet?,' *The Independent*, 6 December 2018. This massive consumption (honestly: waste) allows a maximum speed of 7 (seven) tps (transactions per second), while the enormously less energy-hungry VISA network can handle spikes till to 56.000 tps (Matt O'Brien, 'Bitcoin is teaching libertarians everything they don't know about economics', *The Washington Post*, 8 January 2018). Izabella Kaminska has been writing about this for the *Financial Times* for some years.
[15] Sara Hsu, 'China's Shutdown Of Bitcoin Miners Isn't Just About Electricity', *Forbes*, 15 January 2018.
[16] As an Italian author with deep family roots in the south of my country, I respectfully ask to be believed on my word.
[17] Even if technically feasible, a not very obvious issue.

Futility of Government Bans, Bitcoin Always Find a Way. The rationale is crystal-clear: Bitcoin (and therefore: each pure Blockchain) allows users to get rid of the government, of any government. I do not know if it is superfluous to note that governments do not act only on their own behalf, but also on behalf of their citizens. Resources held in Bitcoin, for example, are effectively shielded against tax authorities, but also against the ex-wife who does not receive the children's maintenance payments: there is no place, physical or virtual, where a seizure may take place. The same would apply to buildings, if they could ever be ruled by a pure Blockchain.

One may already take a stance based on this, but we are not finished: absence of *law* does not mean absence of *power*. On the contrary; a small tour on any Blockchain online magazine[18] will easily wipe out any illusion. Each software needs updates, and Blockchain is no exception. Such evolutions are discussed in decision-making processes led by the major players, and where issues such as the best way to preserve the political balance between miners and other operators are openly discussed. When disagreements cannot be composed, the Blockchain splits into two distinct entities, governed by different rules: they are called *forks*.

A pure Blockchain is therefore not an Empyrean where eternal, immutable and infallible rules protect the rights of each stakeholder: it is an arena whose regulations, rather than being enacted by national or international authorities (as imperfect as they are, but subject to public scrutiny in one form or another) are written down by the members of a new elite of questionable pedigree, some of which could take orders from Beijing.[19] An anarchist's dream and an Orwellian nightmare may be just one step apart.

Permissioned Blockchains

Closed, or permissioned Blockchains, are run according to conventionally established rules; such rules may set the definition of the subjects involved or that may be involved, the methods for entering data, how to resolve any dispute, and so on. The system may be also devised by a single operator, and made open to others.

As a rule of thumb, Blockchains of this kind are immune from the critical remarks presented in the previous paragraph. Professional operators are in the best position to adopt any suitable technical measure in order to prevent any loss of data in the Blockchain. They know how to devise economic mechanisms capable of dealing with system inefficiencies, making use of insurance if needed. People and companies involved are well known beforehand, and therefore the operations will be actually tracked. Covenants will tell to what extent the Blockchain data will be legally binding; in the same way, the business model will be established. Such agreements will follow the common rules of Private International Law, which will identify relevant legal systems or regulations[20] and dispute resolution techniques.

It is hard to deny that a Blockchain is more expensive than a centralized database. It needs multiple nodes, that is many interlinked computers or groups of computers: this alone makes the infrastructure technically and economically more demanding. One needs a good reason to choose it, and the most obvious is the lack of an authority recognized by all of the users. By way of example, consider the world of shipping. If owners of ships and containers, based in different locations such as UK, EU, USA and China, want to launch a tracking system for containers, no one can reasonably aspire to be the sole holder of the legally binding data. Blockchain appears in such a context as an excellent solution, a sort of virtual Geneva of the Internet.

However, Blockchain has often been proposed as a replacement for existing centralized systems.

The most obvious risk here is reinventing the wheel. Blockchain based systems for real estate registers have been put forward. Qualified people, called 'gatekeepers', would check conveyances and other relevant document and properly enter them in the Blockchain. This is not flabbergasting news. Notaries

[18] Such as https://bitcoinmagazine.com/ .

[19] Cooperating with the Chinese is not evil at all, on the contrary, but ultralibertarians are making a quite unsafe bet if they expect Middle Kingdom rulers to support an agenda that is fiercely against any interaction between the state and the economy.

[20] Hopefully international consensus will prevent farces like the tax agreement between Apple and Eire, according to which almost all the profits allocated to Apple Sales International, in Cork, Ireland, were shifted to a head office within the firm. This head office was not based in any country and did not have any employees or own premises; its activities consisted solely of occasional board meetings. I agree without reserve with the bold editorial 'The Guardian view on tax and Ireland: Apple, pay your way', *The Guardian*, 30 August 2016.

exist, and if we want to call them 'gatekeepers', I have no insuperable objection to raise. Land Register are run by civil servants and usually do a good job:[21] I see no particular reason to replace all of them with a different system, since what we have works.

This is not always the case. In the first half of 2018, a decision of Lantmäteriet, the Swedish property registers, made the news: they were studying the adoption of a Blockchain system. Just a few lines beyond the newspaper titles, interesting news about the context of such decision were available.[22] The Swedish Land Register does not follow best practices: their records are months behind, they do not accept electronic deeds and so on.[23] Being well into the twenty-first century and not belonging to any major notarial family,[24] it could indeed be a good idea to adopt a completely new system (based, why not, on Blockchain), establishing an innovative network of 'gatekeepers'. On the other hand, the invitation, addressed to the countries whose only fault is owning well working systems, to throw them away, should be better returned to the sender, unopened.

A conclusion

Twenty years ago the digital signature was surrounded by a formidable aura of enthusiasm, a hype that promoted it as a solution to any identity problem, on the Internet and perhaps elsewhere; in the prologue we have seen how even the President of the United States of America jumped on the bandwagon in a shed close to Dublin. Most of the expectations failed to materialize: the digital signature is a niche tool today; very useful, maybe even vital for some applications, but a niche tool anyway.

Blockchain technology could follow a similar path. I think it will be adopted in some important frameworks: the reshuffling under way in the global power hierarchy is likely to encourage a creative use of Blockchain. Innovative solutions, departed from known paradigms, have greater chances to look attractive in China[25] and elsewhere. On the other hand, I do not think that we are going to live in a *blockchained* world anytime soon. For law professionals, interesting times may be ahead. Permissioned Blockchain agreement must be drafted, and lawyers will face challenging problems, of great variety, complexity, breadth and depth.

Ugo Bechini is a Civil Law Notary in Genoa, Italy

www.bechini.net

[21] In my 25 years old practice as an active Civil Law Notary, I cannot remember of a single customer or professional putting forward the concern of a falsification of the Land Registers' books.

[22] See for example Shefali Anand, 'A Pioneer in Real Estate Blockchain Emerges in Europe', *The Wall Street Journal*, 6 March 2018.

[23] Italian Registers, which I know very well due to a daily interaction, have received online digitally signed deeds since the beginning of the century, and their arrears are measured in hours; similar performances are common in several countries in Continental Europe. Reports of this kind are received with some scepticism, especially in the US: such a claim of efficiency from a country like Italy, not particularly renowned (so to speak) for the respect of law, sounds somehow outlandish. I think that such reasoning should be overturned, upside down. A law-abiding country like Sweden can put up with inefficient Registers (albeit not forever, I'm afraid); elsewhere inflexible systems should better be in place. I will just put the countries I'm going to mention on par with my own, so I hope that nobody will take offence: I do not think it's a coincidence if Colombia and Moldova have implemented some of the world's most advanced digital systems for the verification of documents intended for international circulation (called *e-Apostille*); a search for similar infrastructures in Sweden, Switzerland or Germany would yield no result.

[24] The most important notarial organisation is, in Spanish: Unión Internacional del Notariado (UINL), in Italian: Consiglio Nazionale del Notariato, and English: International Union of Notaries; it federates Civil Law Notaries from 88 countries (https://www.uinl.org/) that count for well over half of world's population. The 'L' in UINL used to stand for 'Latin', but is sometimes skipped now as countries as China, Japan, Indonesia and Russia adopted the Civil Law Notaries system. In most countries, service as a Civil Law Notary is a coveted profession, available only to law school graduates that have received extensive postgraduate training. In Italy, for example, thousands of lawyers (mostly already admitted to the Bar; many of them are tenured judges) convene in Rome each second year for a national exam; an average of 150/200 pass and become part of a professional community that takes pride of the fact that only 0,003 per cent of their real estate deeds ends up in court. On the other hand, Notaries Public, chosen according to a completely different standard, are available in the United States and other common law countries. Small but internationally respected groups of Civil Law Notaries are active in Florida and in the City of London; the latter are known as the London Scriveners.

[25] A general view is offered by Abigail Grace, 'China Doesn't Want to Play by the World's Rules, in Foreign Policy', *Foreign Policy*, 8 August 2018, and for the big picture, see Henry Kissinger, *On China* (The Penguin Press, New York 2011).