The second era of the internet, digital signature infrastructures and trusted entities
KSI, PKI and Permissioned Blockchain

By Eduardo Lacerda

A new era of technology, born on the great platform of digital information, which will still permeate us for some time, emerges and stands out to the avid and anxious eyes of all segments. The new, sometimes, even using contemporary cryptographic forms to support the security in transactions and electronic documents, raises doubts, fears, concerns of not nodding about being the protagonist of the speech and projects or the probable vertical intervention in the business itself of a such innovative theme, not only for transactional asset systems, but also for the directions of societies and governments.

Blockchain, a Chain of Permanent Electronic Blocks or, extending, a Chain of Permanent Electronic Records, or whatever name one gives this, is an ingenious technological procedure for data storage that involves a protocol of trust and consensus on a network, based in the communication and authentication of distributed point-to-point registers, commonly referred to as Distributed Ledger Technology (DLT). It is built by cryptographic block links in order to increase (for some people to guarantee) the tamper-proof mechanisms and in this point, inclusive, the terms inserted in the competence of the illustrious community of digital signatures. There are no secrets in the technological inputs behind this meticulous way of fully registering, with a robust mechanism of immutability, digital assets, which can be coupled with the legal manifestation of will in electronic documents and transactions.

Deceived are those who in an initial reading allow themselves to conclude that blockchain is strictly an anarchic platform, based on an unregulated or non-legislated State, although the procedural genesis, technically elegant, it is tangentially, or more rigorously, it is bound with the non-regulation of transactions in virtual currencies or cryptocurrency, without the need of a reliable third party (probably written in 2008 by the huge subprime crisis triggered in 2007; who knows?). It is a fact that these currencies, even in a legislative shiver and doubts of the regulatory agencies, grow and take up spaces in different segments of society, but nevertheless, governments begin to insert themselves in some way to “regulate” them (will this regulation be possible or is it sufficient to monitor the origin – publication of addresses by the taxpayers to the competent entities and mitigation of masking or mixture issues – and destination, that is, the transactions of the cryptocoins?), as well as the institutions in which they are operated. Blockchain is more than the platform that ensures the transactions of the most known cryptocoins (bitcoin, ethereum classic, dash, zcash, monero, fatcom, among others); Blockchain is a new structure that integrates concepts that will be discussed forward, to guarantee the immutability of registries, confidential or not, public or private, with permissioned authentications and consents or not, which may affect in more or less regulation and should be developed within a Democratic State of Law. In this sense, the UK government produced a glowing report called *Distributed Ledger Technology: beyond block chain*.

It is important to emphasize that initiatives and projects, including those already developed by governments, universities and companies, need maturation, especially in the use of protocols (a topic that deserves a separate article, dealing with the hyperlegder, corda, ethereum – smart contracts, ripple, monero, bitcoin, chain, among others) in which, for each type of business or application, can guarantee privacy, scalability, traceability, temporality and resilience. However, several of these protocols currently known for creating a DLT network are not compatible with the assumptions aimed at ensuring authorship and security in identifying, requesting, generating, issuing and saving the user keys, including authorization and access to transactional platforms. They have their own encryption / signature mechanisms, not allowing other types to the originally shipped procedures in the respective codes. Probably, for applications that are reduced to bilateral transactions – and it is a fact that much of the information society segment is thus combined – this is a viable model, but when it immerses itself in individual guarantees, rights and duties of citizens and companies, there is no certainty about the proper manifestation of will, coming from clear processes of identification and use of digital signatures.

At this point, it is introduced the proposition of this text and the relevant concepts to the role of digital signatures infrastructures and the reliable service providers in this new era. Here, therefore, a concatenated and summarized study on two thematic axes will be carried out: (i) Public Key Infrastructure – PKI and Keyless Signing Infrastructure – KSI and (ii) permissioned blockchain; among many other concepts that will be definitively included in this technological sphere to the technical, legal and normative framework of the digital signatures and accreditation of trusted entities or "miners". It will be a foundation for applications aimed to serve the society (perhaps by building a government blockchain network) and not private, although the same solutions can be used.

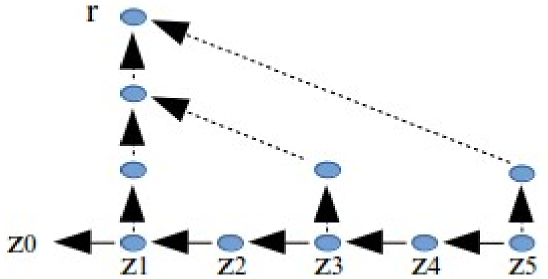
The first thematic axis is about the digital signature infrastructure. There are whispers about blockchain ending with the need of digital signatures/keys or something of the genre in a PKI platform. No, not yet, but most likely it will transmute the segment. Since the cryptocurrencies platforms use some key generation and key collection models, including to calculate the "addresses" of the nodes, to sign or to give confidentiality in the transactions, it is possible that the mentioned terminating perception is linked to what has been done by the government of Estonia and studied by Digital 5 – D5 (United Kingdom, South Korea, Israel, New Zealand, Estonia and the United States as an observer), which is the use of a KSI. To undo possible confusion, follow the words of Ahto Buldas, Andres Kroonmaa and Risto Laanoja, in the article *Keyless Signatures' Infrastructure: How* *to Build Global Distributed Hash-Trees*: "*The word keyless does not mean that no cryptographic keys are used during the signature creation. Keys are still necessary for authentication, but the signatures can be reliably verified without assuming continued secrecy of the keys.*".

Initialy, KSI is a disparate solution, with other attributes, and also complement to the so-called PKI. Note: alternative and not peremptorily substitutive. *"KSI is intended to protect integrity of an asset while PKI is intended to protect its confidentiality. These are different attibutes."*, from the whitepaper *Keyless Signature Infrastructure® (KSITM) Technology – An Introduction to KSI Blockchain Technology and Its Benefits – Guardtime Federal, LLC Proprietary*. KSI is an infrastructure, in short, using few words, of a hash-tree based time-stamp. KSI congregated, for example, systems structures such as the Gateways, Aggregator, and Core Cluster associated with a Calendar Network which aim to, in addition to allowing integrity and scalability, with "n" keys being generated and only used at a given moment, guarantee the temporality and authenticity of the digital signatures "without needing" (and, here, the quotation marks is an expression force) of a reliable time server, a Certificate Authority, Certificate Revocation List – CRL or Online Certificate Status Protocol – OCSP, among other elements of a PKI network. The truth is that KSI is a great Trusted Service Provider, in which keys and signatures are generated by means of a cryptographic algorithm, based on an application server, and which, due to their mathematical theory and procedures, guarantee temporality, scalability, less damage in the event of a compromise of the generated keys and protection against possible quantum attacks (another theme in this scenario that deserves a further reflection). Question: does it replace a PKI platform?

Instead to what Martin Ruubel states in his publication *Privacy and Integrity on the Internet of Things. If all you have is a PKI hammer…*, which he wrote: *"After the invention of PKI a separate use case was proposed – digital signatures i.e. by signing data with a private key then others can verify the integrity of the data using the signer's public key. There are many problems with this. The first is that the proof of integrity is more of an attestation, i.e., it is true only because the signer says it is."*, the Brazilian Public Key Infrastructure – ICP-Brasil – adds several functions for private key protections, from technical and procedural requirements for the Certification Authority, to the indelible connection between it and the physical person (including the current prerogative of the modern and substantial biometric system of ICP-Brasil, unique in allowing different biometric technologies to be integrated in a safe, anonymous, online, distributed – without a central database – and with the guarantee of uniqueness of all records), and here lies the irrevocable premise of the exclusive control and use of the private key by the holder, that is to say, the guaranteed manifestation of will, technical and legal, given to the boundaries of MP 2.2200 / 01 (Federal Law which created ICP-Brasil) and the technical norms associated. At this moment, it is increased to the mathematical functions of public and private key generation in RSA, still the most used algorithm in the Brazilian infrastructure (gets registered that the ICP-Brasil V4 chain is based on the ECC-Brainpool r1 suite) the physical and logical security procedures of this infrastructure, highlighting the rigor of its processes of identification, request, generation, emission and storage of the private key. In the hermeneutics of its norms, in addition to the paragraphs of its legal dictum, we will find postulates that produce a fully (stands out by the light of the Value of Evidence Theory) legal validity to the digital signatures made in documents, assets, transactions and, as well as, digital authentication, that is, without needing of another mechanism to prove its authorship, integrity and authenticity, which, together with a reliable structure of time, also regulated by ICP-Brasil, gives perenniality to any digital signature. One part: highlight the importance of the technical and legal distinction between digital signatures and "electronic authentication", such as "user and password" or biometric signature – which serve only for authentication reasons, with specific niche of performance, and do not currently have the mathematical, procedural, security, and, therefore, legal characteristics of a digital signature.

In view of the above, how can KSI blockchain technology help? In everything. KSI, for example, can deliver, on its own, temporality to the digital signatures of ICP-Brasil. As Trusted Service Providers, due the regard to the applicant's will and self-expression, these two infrastructures can be used mutually, since: "*In a keyless signature system, the functions of signer identification — and of evidence integrity protection — are separated and delegated to cryptographic tools suitable for those functions. For example, signer identification may still be done by using asymmetric cryptography but the integrity of the signature is protected by using keyless cryptography — the so-called one-way collision-free hash functions, which are public standard transformations that do not involve any secret keys.*", from the mentioned article. However, it is necessary to create a technical, procedural and legal environment to give full effect to these digital manifestations. In spite of the fact that the debates are fundamentally focused on the problem of the private key compromise on a PKI solution (not ignoring, subscribes, questions of vulnerability of signatures to quantum computational attacks, the "complex" revocation system and confirmation of authenticity / integrity to a PKI, based on RSA, for example), in order to avoid premature disclosure of the KSI key (see below an example of key generation in the BLT algorithm, extracted from the cited article), extremely strict procedures are required, such as the maintenance of a dedicated cryptographic device to generate the random seeds, strong security and clear communication between the client application and the KSI server, as well as the configuration of the Hash-Calendar structure (for example, hardware apart), as well as a strong identification of the client and server sides. Finally, it is necessary to create a Trusted Service Provider for this type of digital signature (which can induce procedures for qualified and non-qualified certificates, following the European regulation).

It is fundamental to consider at this moment of massive advances in projects of Internet of Things – IoT (and even in these cases, it is essential to address the issue of equipment identification), scalability in digital signatures, resistance to quantum attacks, among others, a discussion addressed by the government of Estonia and its service provider (Guardtime – BLT based KSI blockchain technology) on the change in the mathematical foundation in this cryptographic framework. In this envelope, to illustrate, the BLT algorithm is shown.

Key Generation	The client-side device generates a random seed z_s. For each unit of time t, the client application generates a password (one-time-password). The passwords are calculated by using $z_{i-1} = f(z_i)$, for each $i = s \ldots 1$, where f is a hash function, building a hash key chain. $z_0 \leftarrow z_1 \leftarrow z_2 \leftarrow . . . \leftarrow z_s$. The client-side also calculates the root hash r of the merkle-tree, as shown below:  The public key is given by $(z_0\ e\ r)$ and it is sent to the signature server. The server will only get to know z_{i-1} when the client application uses it, but as the server knows z_0, the password could be verified by the relation ~~a~~ $z_{i-1} = f(z_i)$.
Public Key Certificate	The public key certificate sent to the signature server will be: (IDc, z_0, r, t_0, IDs), which IDc is the client side identifier, t_0 is the time unit that the certificate became valid, IDs is the authorized signature server identifier. For revocation, just send a revocation message to the signature server of this certificate.
Digital Signature of a Document	To sign a m message (compute the hash of m), which $t > t_0$: the client computes $x = h(m, z_i)$ and sends x with IDc. The signature server verifies if the client certificate was not revoked and creates a time stamp based on a hash tree $S_t = (x, Idc)$, than it sends it back to the client side. The message signature~~s~~ is (IDc, i, z_i, c_i, S_t), which c_i is the proof that z_i is in the i position of the hash chain of keys.
Signature Verification	To verify a signature (IDc, i, z_i, c_i, S_t) of a m message: The client identifier must be the same as the certificate's identifier. With the z_i keys and the hash chain it should be possible to mount r. S_t is a valid time stamp in $(h(m, z_i), IDc)$. The t time of S_t satisfies $t = t_0 + i$. The signature server identifier in S_t must be the same as the certificate's identifier.

Conclusions of the first axis:

(i) the content of the previous paragraphs, in this small technological description, will affect the basic structures of a PKI, consequently, of course, the ICP-Brasil. When and to what extent? Difficult to answer.

Note 1: There are projects that use ICP-Brasil digital certificates and others that model a PKI blockchain structure, as can be found at the websites below:
-http://idgnow.com.br/internet/2017/05/25/empresas-ja-podem-usar-blockchain-para-validar-documentos-juridicamente-no-brasil/
-http://www.the-blockchain.com/2017/06/17/wisekey-partners-blockchain-interface-company-riddlecode-develop-innovative-solutions-securing-iot-via-blockchain-technology-crypto-hardware/?ct=t(RSS_EMAIL_CAMPAIGN).
-https://valid.com/pt-br/what-we-do/digital-certification/blockchain/

(ii) it becomes increasingly necessary a new and wide regulation of a national system of a digital signature and identification (for Brazilian purpose), with several models, hybrids or segregated, that will be executed to the extent of a law that is consistent with the future of digital signatures, identifications and assets.

The second thematic axis is about permissioned blockchain and a reference construction for trusted entities or "miners". The word "permissioned" in this context means a restriction of the network to those who can participate in the consensus mechanism in the construction of a blockchain legder, that is, an unambiguous and transparent identification of whose are the addresses that expressly have authorization to authenticate the blocks transactions and / or calculate a certain consensus mechanism. By broadening the understanding, it can even determines which point is allowed to create smart contracts (in an application requiring multi-services) or even endorse them, thinking about regulatory entities or segments of society in which the assets must be sanctioned by the will of the law and the transaction itself in a blockchain network. In this discussion, questions about the return of centralized databases arise; it is not enough, but, undoubtedly, getting to know the respective business, including the impact on the storage of the data in distributed blocks, will determine what type of technological approach should be done, including on the subjects already mentioned, as authenticity, privacy and scalability.

Note 2: It is noteworthy that several recently published articles and news attempt to solve the problem of identification in a blockchain network (decentralized identities assignments and network hubs); the guarantee of digital expression is not simple. ICP-Brasil addresses this issue in an exemplary way and increasingly becomes a worldwide reference in the business of a digital and dynamic identification – see the citation in the public hearing of the Trade Commission, Science and Transportation of the American Senate, which can be found on the website: https://www.commerce.senate.gov/public/_cache/files/9348f11b-49a4-4c47-922e-f5cc98d61b54/469C33D81041FAB151DC6B1E6608A18B.11.08.2017---wilkinson-testimony.pdf

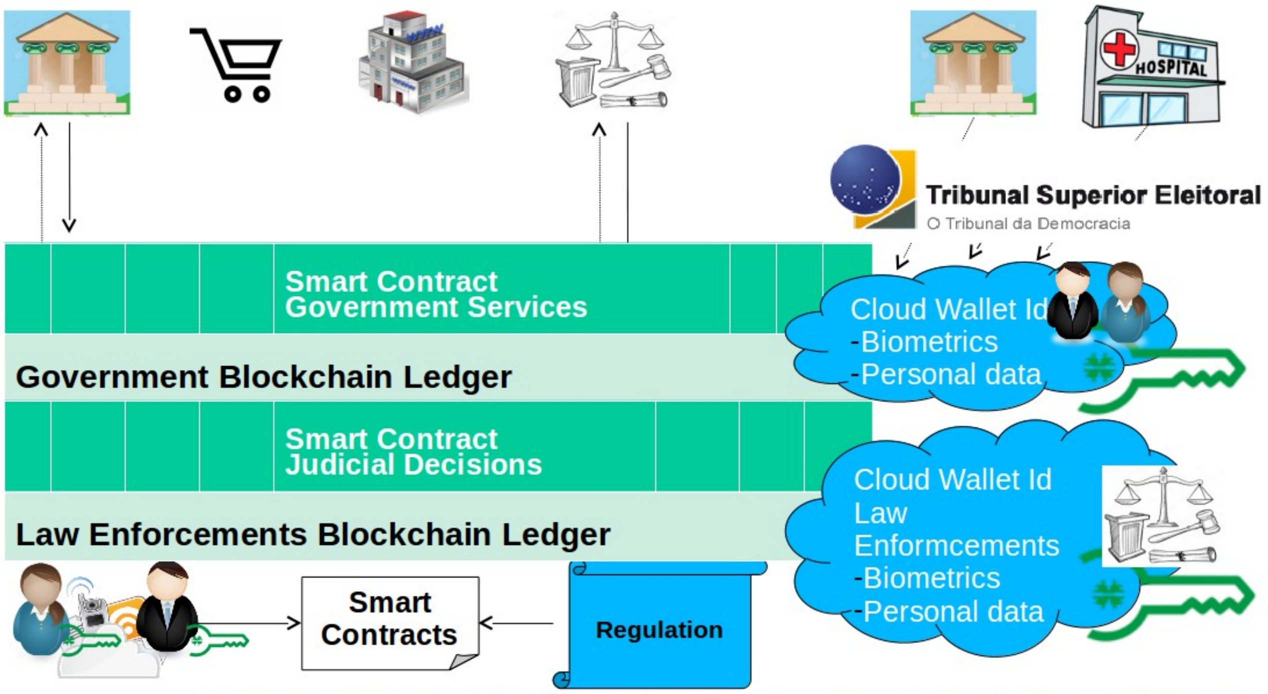
It is based on the premise, for the purposes of public interest and individual guarantees, that any approach of DLT, blockchain, smart contracts, among other concepts, should be followed by a regulation and authorship of the expression of will, in a State which configures the power in a tripartite form (especially to a sphere in which the citizen can appeal), emanated by a positive right and with democratic rules. The first thematic axis technically discourses this need. In this second one, intertwined with the creation of a coherent legislation, the minimum conditions of safety and efficiency must be created so that applications, mainly governmental ones, can, at first: (i) comply with the current laws and future adaptations and (ii) supply the information society with safe and efficient services. It is true that a blockchain government network needs to address problems related to identification of its citizens and companies, information privacy and solve the nuances of the protocols scalability using methods such as Proof of Work – PoW – and Proof of Stake – PoS. In the latter theme, follows the comment of Vitalik Buterin, founder of Ethereum, on the website https://blog.ethereum.org/2017/04/01/ethereum-dev-roundup-q1/: "*After three years of trying to find solutions to the "nothing at stake" and "stake grinding" attacks, we have decided that the problem is too hard, and secure proof of stake is almost certainly unachievable. Instead, we are now planning to transition the Ethereum mainnet to proof of authority in 2018 (...).* On the website: *https://ethereum.stackexchange.com/questions/13968/are-miners-eliminated-in-proof-of-authority/13969,* follows: "*For those not aware of how PoA works, it's a very simplistic protocol, where instead of miners racing to find a solution to a difficult problem, authorized signers can at any time at their own discretion create new blocks.*".

In a non-permissioned network, based on PoW, all nodes redundantly participate in a race to solve a puzzle and authenticate the transactions (blocks). The miner that solves the consensus rule is rewarded (as long as there is a reward – it is important to understand the possible problems of rate increases, for example, in a bitcoin application or fees from a smart contract) and the new block is distributed to the network. As it is known, a tremendous computational effort is consumed by several nodes, and only one of them will arrive at the expected result, and thus the effort (time and cost) made by other points will be wasted. Adopting PoS, lies on the problem of self control and ability to adopt network criteria.

In the opposite direction to this scenario, a permissioned network, besides not coexisting with the problem of the diminutive reward, may have more efficiency in the computational tract for a given application, since criteria, methods and computational structure can be established for known "miners", which should only focus on the resolution of issues pertaining to that application. Futhermore, updates and evolutions in the consensus protocols can be established more quickly, since within this transparent consortium, mainly for a government directive, timely solutions (obedience to the regulatory acts) are done to a possible impasse in detriment of a non-permissioned network. It is important to emphasize that it is fundamental to knowing the business to which one intends to build a permissioned network or not (even the need to use a DLT blockchain platform). There are many applications, such as open-data queries or supply chains, where there are registry integrity needs, but not scalability, which may be non-permissioned networks, adopting the possible rewards and consensus criteria, however, when society demands efficiency and security, with the dependence on the delivery of a right or the collection of a duty, permissioned networks fit better.

This view makes this transparent consortium of known addresses, whether governmental entities – which already have such assignments – or the private sector, in trusted "miners." From a given application, the government can regulate and accredit (and all processes arising from such an act – disclosure, maintenance, and auditing of addresses, systems, methods, and cryptographic schemes) that will attempt to authenticate the data or, if necessary and regulated, the appropriate actions for the citizen, companies and spheres of the state in a legder, with regulatory security and the technology itself – without the need for a centralized data bank. In this scenario, the development or the possibility of using open, mutable and auditable codes are essential. The National Institute of Information Technology (www.iti.gov.br) of Brazil – ITI – has in its mission to accredit, audit and supervise reliable entities. It is part of ITI nature to lead this path.

A model suggested by this text is the creation of a government blockchain network, in which several services – critical, open-data, consultative, contractual, beneficiary, private – are established and protected by user keys (and their usage and subscription models), allowing access to individual data, smart contracts (authorized to trigger multiple services) regulated and sanctioned by inspection entities or established by law, registering all the acts and assets in a government legder. In this context, it is fulfilled all the criteria of authorship and the due manifestation of will, integrality in the documents and transactions, immutability and perpetuity, where relevant, of the records and privacy in the data and contracts in which the legal rule thus endorse it. All segments of society and government could appropriate from this network without the need for replication of infrastructures and data, without central databases, with the institutional security granted by trusted entities in a permissioned blockchain network.



Concept: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector; Source: www.br.depositphotos.com

For ICP-Brasil, although there are several other possibilities mentioned in the first thematic axis (another example: a blockchain platform for transparency of SSL certificates – positive domain registration), there are two interesting and newsworthy scenarios. The regulation of Trust Service Provider – TSP and a platform of Know Your Costumer – KYC. In this first area, standards were written which describe the key storage concepts of end users in HSM, with interoperability due to use of the Key Management Interoperability Protocol – KMIP, and the digital signature service (signature / verification portal and storage of electronic documents – reference: eIDAS 910/2014 and associated directives). There are established for online digital signatures, which the keys will be hold in trusted entities that will be able to store thousands of millions of documents digitally signed, that is, adequate environment to structure a ICP-Brasil Blockchain Ledger project. In-depth studies of which platforms and protocols to use (or the development of one with universities, companies and governments) should be done, but certainly will be the thrust for other projects, not only in ICP-Brasil, but also for Brazilian State. The second one, given the ICP-Brasil Steering Committee resolution 131, of 2017, which allows the use of applicants biographical and biometric data, is to create a ICP-Brasil KYC platform, studied by several segments. With the use of a ICP-Brasil digital certificate, providing privacy, security and legal guarantees, illustrated in the figure above, accredited entities could make consensual use of customer data, ensuring irreversibility of any access, perennial for the entire chain.

Therefore, the creation of a DLT blockchain network should be planned and necessary. Studies and maturation are the scenarios that currently permeate all governments, companies, academic environments and citizens, with a purpose to review the business line concept and for what this new technological platform will be useful. In fact, applications and protocols evolve (at great strides) and seemingly is a path of no return, given the size of investments and the segments of society that are building models for assets transaction and registration, deployment of services and payments, confirmation of supply, creation of identity concepts, among others in this new era of technology. Concurrently, digital signature infrastructures will change and it is necessary to keep the pace with what has been studied by other governments. Permissioned network for public applications that affects the individual~~s~~ rights and duties before a society seem to be the path to be trodden. Opportunities are hatching and do not collide. Knowing the business – risks and opportunities – that is the key to development.

References:

Blockchain for Identity Management
by Ori Jacobovitz, Technical Report #16-02, December 2016

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World
by Don Tapscott & Alex Tapscott

Cryptocurrencies, Blockchains, and Smart Contracts
by Arvind Narayanan and Andrew Miller

Distributed Ledger Technology: beyond block chain
A report by the UK Government Chief Scientific Adviser

Distributed ledger technical research in Central Bank of Brazil – Positioning report
Technical consultants: Aldenio de Vilaca Burgos; Jose Deodoro de Oliveira Filho; Marcus Vinicius Cursino Suares; Rafael Sarres de Almeida
E-mail blockchain@bcb.gov.br
Research Manager: Aristides Andrade Cavalcante Neto
Chief Information Officer: Marcelo Jose Oliveira Yared
Authorized by Deputy Governor: Luiz Edson Feltrim
Central Bank of Brazil

Efficient Implementation of Keyless Signatures with Hash Sequence Authentication
by Ahto Buldas, Risto Laanoja, and Ahto Truu

Efficient Quantum-Immune Keyless Signatures with Identity
by Ahto Buldas, Risto Laanoja, and Ahto Truu

Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees
by Ahto Buldas, Andres Kroonmaa, and Risto Laanoja

Oward a philosophy of blockchain, Introduction
by Melanie Swan and Primavera de Filippi, Guest Editors

Proposta de uma Infraestrutura de Chaves Públicas construída sobre o blockchain do Bitcoin
by Antônio Unias de Lucena, Marco Aurélio Amaral Henriques

Sovrin Provisional Trust Framework - Sovrin Board of Trustees, 28 June 2017, Sovrin.org

State Management for Hash-Based Signatures
by David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann

The iEx.ec project Blueprint For a Blockchain
based Fully Distributed Cloud Infrastructure, White Paper, March 18th, 2017, Version 2.0, Release Candidate

The Truth About Blockchain - It will take years to transform business, but the journey begins now.
by Marco Iansiti and Karim R. Lakhani

Using the Blockchain of Cryptocurrencies for Timestamping Digital Cultural Heritage
by Bela Gipp, Norman Meuschke, Joeran Beel, Corinna Breiting

Websites:

http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract/

http://www.the-blockchain.com/2016/04/13/smart-contracts-the-good-the-bad-and-the-lazy/

https://www.law.ox.ac.uk/business-law-blog/blog/2017/04/how-blockchain-technology-will-impact-digital-economy

http://yalejreg.com/nc/the-firm-as-a-nexus-of-smart-contracts-how-blockchain-and-cryptocurrencies-can-transform-the-digital-economy-by-christian-catalini/

https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

https://www.ethereum.org/

https://www.hyperledger.org/

https://www.r3.com/

https://guardtime.com/

https://www.coindesk.com/5-blockchain-developments-coming-2018/

https://blockchainhub.net/

https://www.evernym.com/

https://bravenewcoin.com

https://www.forbes.com/sites/jasonbloomberg/2017/10/06/can-blockchain-solve-the-quifax-identity-moass-heres-how/#bd05438296a7

https://br.cointelegraph.com/news/blockchain-digital-identification-in-canada-coming-in-2018

https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scan-canadians-to-use-blockchain-for-digital-ids