BLOCKCHAINS UNCHAINED: The Implications of Blockchain Technologies for the Public Sector

Draft Working Paper (Second Half)

Observatory of Public Sector Innovation

Reform of the Public Sector Division (RPS)

Directorate for Public Governance (GOV)

OECD

26 February 2018

Prepared by Théo Bourgery, Intern, opsi@oecd.org

This draft paper is shared online on the OPSI blog (http://oe.cd/opsi-blog) for public comments from 26 February 2018 through at the 20 March 2018. Interested individuals are invited to REVIEW and COMMENT on the paper **by 20 March 2018** through the collaborative document at http://oe.cd/blockchainunchained or by editing the document in tracked changes and emailing revisions to opsi@oecd.org.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

public sector are numerous, they are not always evident. It is *not* the case that Blockchains answer all of governments' problems. The next section seeks to make sense of such challenges and understand where technological limitations lie.

Transparency, Confidentiality and Decentralisation

Public Blockchains allow for perfect transparency, where "decentralised architectures generally rely on the disclosure of everyone's interactions" (DeFilippi, 2016, p.1). Confidentiality settings are close to non-existent. Yet confidentiality and privacy mechanisms, at a time when the storing of personal information becomes more likely, are of paramount importance. Rules and laws insist on the absolute protection of such information. This is particularly well exemplified by the EU's right-to-be-forgotten principle, which stipulates that an individual may ask to have her record deleted from government databases (see Gabison, 2016).

A necessary trade-off will have to be struck between levels of decentralised decision-making and privacy settings. Higher levels of privacy will require more centralised governance models (permissioned Blockchains) while "radical transparency" (DeFilippi, 2016, p.0) will bring risks to the exploitation of personal data, but remains closer to the Blockchain technology's underlying aim to function independently of centralised authorities.

Coding and Governance Models

Who, or what, is the legitimate governing entity of Blockchains, be it public or private? As greater accountability on all spheres of public life is demanded by civil society, decisions over who controls Blockchains is of importance. DeFilippi & Loveluck (2016), in the specific context of the Bitcoin platform, decipher two layers of coordination:

- "The *infrastructural layer:* a decentralised payment system based on a global trustless peer-to-peer network which operates according to a specific set of protocols;
- Layer of *architects*: a small group of developers and software engineers who have been entrusted with key roles for the development of this technology" (p.10).

Levels of decision-making, and the integration of such decisions in the platform's code, are thus contingent on… the code previously drafted. Power dynamics, even in public Blockchains, are ultimately constrained in what the code of each and every platform allows for.

As governments bring their attention to Blockchains and further development occurs, it might be that there will need to be an added focus on the level of government intervention versus room for a consensus-based way forward. It will ultimately require government entities to be familiar with the process of coding, and constrain room for change on the platforms to what is deemed feasible and democratically acceptable.

Talking About Blockchain – Separating Blockchain from *Bitcoin*

There seems to be a large consensus across Blockchains specialists that *talking about Blockchains* to citizens is one of the most complex part of their jobs. In the words of Justin Herman (2017), Emerging Citizen Technology Programme Lead at the US's General Services Administration, "The technologies of Blockchains are supposed to increase trust. And yet, […] either within Government or within the Blockchain community itself, there is an inherent distrust. That's one of the most important things we have to work on". Similarly, Tomicah Tillemann (2017), co-founder of the Blockchain Trust Accelerator at the *New America* think tank, considers the lack of education about the technology to be one of the main hurdles facing the Blockchain community: "Blockchains are technologies that are very misunderstood, it is complicated technology. We spent a year and a half with some of the best thinkers and the best communicators in the World, trying to come up with new strategies for explaining the technology. We have made some progress there, but the basic reality is that this is not a simple technology".

At the same time, Emmanuel Noah (2017) of BenBen speaks quite differently of his introduction of Blockchains to senior public officials: "What spoke most to the authorities when we introduced our Blockchain solution were the benefits that the solution brought in terms of public service delivery, along with the possibility to maximise revenue generation […]. The Government has revenue targets, customer satisfaction reviews – these were the main arguments we used with the Government". On a rather different page still, Mats Snäll (2017) of the Land Registry Authority argues that he "should not be forced to explain [Blockchain technologies] because no one should even care about that. By essence it is complicated to explain a technology if you are not a technician. You are not asked to explain how a medical diagnosis works if you are not a doctor."

Along with this defiance, and almost paradoxically, the expansion of the *Bitcoin* platforms has been significant in recent years – in terms of market cap, value of the *Bitcoin* against the US Dollar, or the number of recorded daily transactions. More may need to be done to explain and convey the possibilities before blockchain technology can be used widely and become accepted.

Copyrights

Copyrights can be apprehended from two different perspectives when integrated to any Blockchain architecture:

As content becomes so multidisciplinary and copyright ownership blurs, Blockchains are excellent tools to "timestamp [artists' and content producers'] work, keep a 'vigilant' eye out for anyone violating their copyright, create a permanent record of their work and issue their clients a time-stamped copyright certificate" (Willms, 2016). In this sense, they also serve as proof of ownership and proof of existence.

On the other hand, "[o]nce a copyrighted work of art is recorded on the ledger, it will become virtually impossible to take down because no central server can be disconnected and no individual can be stopped." (Gabison, 2016, p.6). Any erroneous information, if confirmed on a blockchain and added to a secured block – for malicious purposes, but also due to nodes' ignorance – will indeed not be mutable or destroyed.

This is of issue in legal terms – who then will be penalised for the provision and use of illegal content? While original infringers (illegal providers of content) may be held liable – and will most likely be more easily traceable than in the current system – they may quickly become judgment-proof. This is particularly true when "a copyright holder attempts to recovery for every download for each upload" (*ibid.*), making original infringers unsolvable in front of Justice. Instead, copyright holders may be more inclined to file injunctions to block access to links rather than *deleting* such links (Gabison, 2016, p.7) – thus going after subsequent infringers (illegal content users) instead. At the same time, it may prove necessary to think of new governance mechanisms to control what goes into Blockchains with regards to protected content – in the form, for example, of accredited observers.

Public-Private Partnerships

The numerous communities of practice that are emerging across administrations share an effort to bring public agencies and private firms together in developing Blockchain systems. Large consortiums such as *R3* or IBM's *Hyperledger*[1], but also the Crypto Valley Association in Switzerland, the Blockchain Trust Accelerator in the US, or the Blockchain and Virtual Currency Association of India aim to bring all actors into one same community with similar goals and aims with regards to Blockchain. In an interview with the Observatory, Justin Herman, who heads one such community of practice, explains that "public-private partnerships [*PPPs*] are not only desired; they are encouraged" (2017). Since the creation of the Global Blockchain Council in early 2016, 15 Blockchain-related projects have seen the light of day, a large majority of which are PPPs (Raford, 2017). More specifically there seems to be a trend where private firms *assist* government agencies with the technological aspect of the work. The most influential model of PPPs in this sector is most likely to be the *ID2020* initiative, which aims to provide a digital identification to all refuges and stateless individuals through signed partnerships with UN sister agencies and private companies such as Microsoft and Accenture.

This rapid development in PPPs, and stronger links between private and public spheres, is also due to the lack of subject-matter knowledge *within* governments. While there is understanding around Blockchain at different levels within the public sector, coding proficiency remains limited. In the words of Axelle Lemaire (2017), talking about the French administration, "we would have to hire data scientists with salaries that compete with that of private companies. This is simply impossible". *Smart Dubai*'s office, acknowledging the issue, has provided 14,000 civil servants with data literacy courses.

Costs and Scalability

Higher short-term costs associated with a still-emerging technology prevent its widespread use for the time being. While these costs are particularly daunting for firms, the political nature of government-run blockchains must also be taken into account as initial investments are discussed, and cost-benefit analyses are run. As found in a number of studies, "running costs associated with the adoption of DLT/Blockchain are as yet unclear" (Deshpande *et al.*, 2017, p.15). Limited long-term visibility over the feasibility of blockchains also remains: "currently, the return on investment for businesses is unclear, which could make it more difficult to argue a case for investing in DLT/Blockchain solutions" (*Ibid.*, p.16).

Conclusions and a way forward

The aims of this short guide were threefold:

- *Explain* what Blockchain is;
- *Explore* what is already occurring in the Blockchain space for the public sector;
- *Make sense* of its impacts on the public sector, and *anticipate* future developments.

It is no easy task – Blockchains are, by essence complex tools, and the existing literature focuses more on its technicalities than its implications in "the real world". Furthermore, the technology is closely related to the infamous *Bitcoin* platform, and splitting the two is now more than essential.

At the same time, the infrastructure has "immense powers" (Rinearson, 2017) that are waiting to be unleashed. More specifically, "the key advance from Blockchain technolog[ies] is distributed trust – removing the need to rely on a specific single trusted third party [...] to facilitate transactions" (Hanson, 2017). The public sector could reach levels of data security never reached before – in fact, it may be the case that data can be *perfectly* safe through Blockchain technologies.

As the technology grows in its applicability and services, it is of paramount importance to introduce and analyse the matter in an objective way, irrespective of what debates in political and civil society scenes there may be – while not becoming insensitive to them. This report has aimed to strike the right balance between those two conflicting forces.

Section I focused solely on explaining the technology in what we believe to be accessible ways. It presents its main features and contextualises Blockchains: how it develops on specific platforms, the rise of Smart Contracts and the security protocols necessary to ensure information on Blockchains cannot be tampered with. It provides the necessary tools to best understand why, and how, Blockchains act as hypersecured ledger which allow for transactions without the certification of an official, trusted third-party – indeed, the very trust shifts from the central authority to the *system* and the consensual decision-making process that it allows. The credibility and security of any Blockchain-run platform is fully contingent on the reliability of actors to take the right decision at all times.

Further, we made clear that the mathematical construction of the Blockchain through a mere chain of blocks of transactions allows for ability to have an immutable history of changes. This is particularly important in a digital era which allows for untraceable changes to any document, thus affecting the very notion of truth.

Section II moved from the technicalities to the implementation of Blockchain services in, and for, government. A number of case studies were presented to have a better grasp as to what the technology truly *means* for the public sector.

Section III is a logical follow-up of Section II, for it seeks to bring a more thorough understanding of what it means for government sectors to be disrupted. On a number of topics, it looks at the challenges of the technology – be it from technical, regulatory or governance aspects. It leads the way to the conclusion that despite its potential great impacts, Blockchains face numerous challenges, from a policy perspective, that concerned stakeholders must address relatively urgently. It is now the work of regulators to understand the technology to protect sensitive information on the one hand, while leaving room for innovation and trying new things on the other.

A number of other questions are brought to the fore as a result of this guide: how will regulation adapt, and at what pace? How will the technology develop – and towards which ends? Will the growing political willingness be sustained – even as the technology requires the redefinition of State prerogatives? Will public servants and citizens-at-large be willing to adopt the new technology? Finally, will there be cases and situations in which Blockchain will *not* be the answer – which implies that cost and benefit analyses must adapt to the new tool?

These are hard questions to find suitable responses too – only because it would come down to betting against the unknown. However they are important questions that one must bear in mind as Blockchains develop and enter the realm of the public sector – and public life.

It is not enough to push the issue away in light of its technical complexity. It is not enough for regulators and policy-makers to give all powers to developers on mere grounds that “they understand it”. As Blockchains develop and may indeed become the new Internet, a lot of work must be done to make such technologies accessible to all, and its impacts on the public sector investigated and known. The rise of Blockchains must not override the necessity for experimentation and evidence to ensure that it is relevant and that it meets the criteria of confidentiality, security, decentralisation to only name a few –

along with the creation of some form of government-wide governance framework. This has never been done in the realm of the public service for Blockchains. This guide is a first step in this very direction.

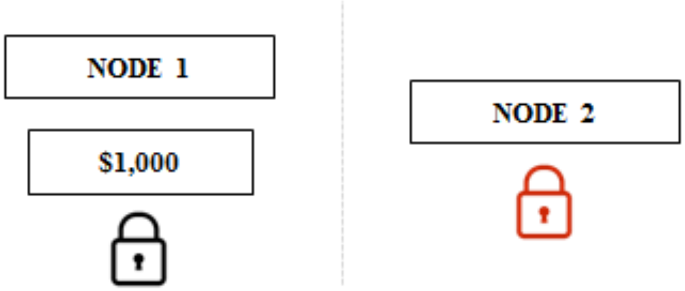
Appendices

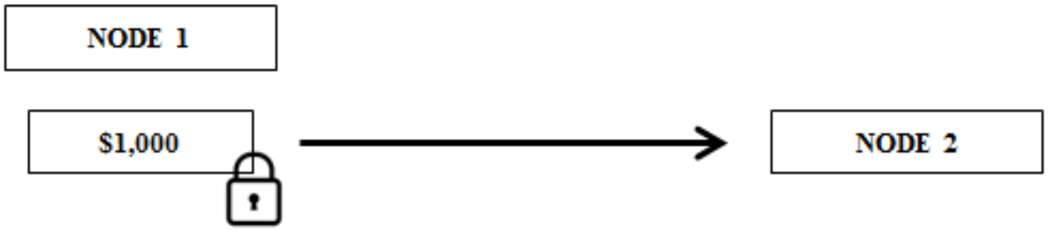
Appendix A: Public and private keys

Public and private keys are a cryptographic protocol that confirms or infirms the identity of each party in a Blockchain-based transaction. Indeed, the mere nature of a distributed system allows for two parties who have never met to transact. Further they must do so without the approval of a centralised third-party, as discussed in Section I.

Public and private keys are not unique to Blockchain technology – in fact they are a rather common protocol to secure information travelling across an unsafe environment. Furthermore, they are prone to change as more efficient protocols see the light of day.

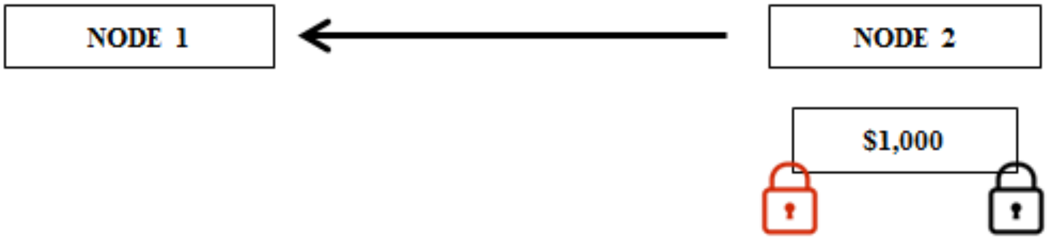
We will start with the assumption that the two parties actually *know and trust each other*. More specifically, each party knows it is dealing with the correct second party, in which it can place its trust. Let’s now assume that the first party, **Node 1**, wishes to transact $1,000 to **Node 2**. Both have padlocks with the corresponding key, and each only has the key to her own padlock, such that[2]:

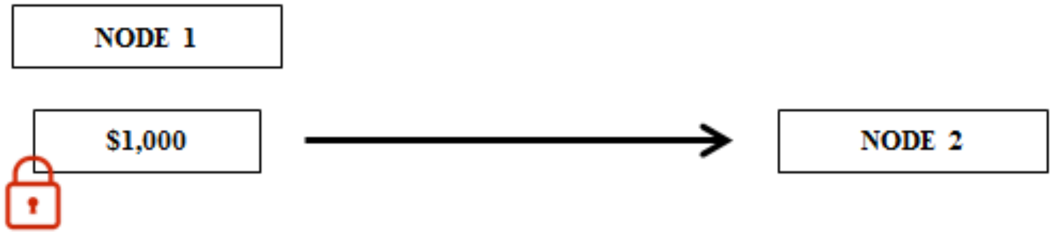




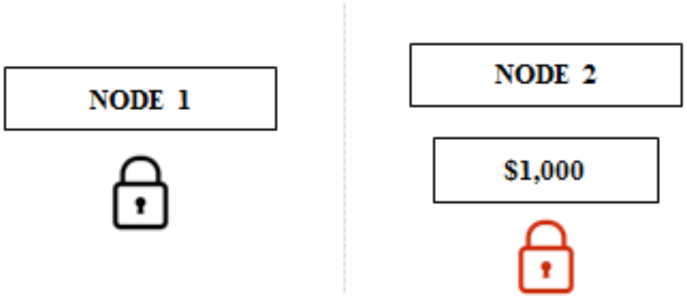
In order to start the transaction, **Node 1** will send the $1,000 to **Node 2** – say, in the form of a sealed package – with **Node** 1's padlock. This ensures that the transaction can securely reach the second party.

Once successfully sent over, **Node 2** will add her padlock to the package and send it back to **Node 1**.





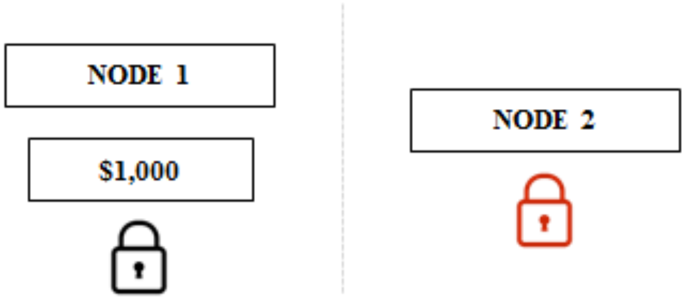
Upon reception, **Node 1** unlocks her padlock and sends the package back to **Node 2**. The latter is then able to unlock her padlock and terminate the transaction. Note that the process remained secured at all stages.

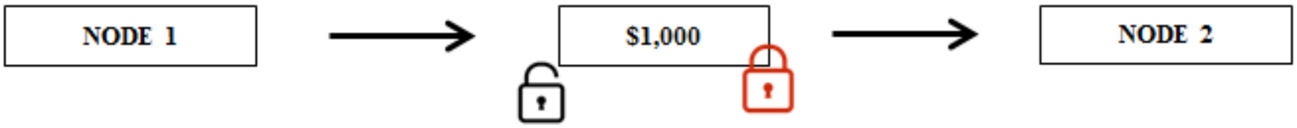


The problem is naturally different when information about one of the party is not perfect. This is particularly relevant when a transaction is sought with a party with whom there was no prior interaction. There must be a way to shift the trust logic from the party to the system. This is the problem public and private keys successfully resolve.

Public keys are cryptographic padlocks in the form of complex strings of numbers, unique to each actor in the network. These can be viewed by all nodes but can only be unlocked by their owner through the means of a unique private key. This acts as a signal that the actor one wishes to transact with *indeed is the actor one wishes to transact with* – ultimately replacing the role of the bank to confirm the identity of the parties.

When a transaction is sought, **Node 1** will forward the correct amount *along with her public key and that of **Node 2*** – thus determining in a unique fashion who the transaction targets. This is not all: **Node 1** will prove her identity by unlocking her public key with her private key (that she only has access to). This acts as a signal that the two parties are indeed fit for transaction.





Appendix B: Hashing

Hashing is the process of compressing any input – a video, written document, a piece of music, etc. – into a mathematical cryptographic output, a hash, of a fixed size. The document essentially becomes a line of numbers and letters, and is *unique* to this document: such that a same input will always produce the same hash[3], and no other input will ever give the same hash. The input is processed through a hash function, which translates as some mathematical equation.

To better clarify, a small paragraph from the Observatory's website will be used as an input to be hashed:

Input

The OECD has developed an Observatory of Public Sector Innovation (OPSI) which collects and analyses examples and shared experiences of public sector innovation to provide practical advice to countries on how to make innovations work. The OPSI provides a place for sharing, discussing and co-creating solutions that work

Once processed by the hash function, it provides this hash:

Hash

9bb11726ad25d7deb9fe1bcebca51550d19c7cb80d2170a7ca6e8e95f18e5763

This output acts as a *digital fingerprint* of this specific input. Not only is it unique, but a minimal change in the input will provide a very different output. Thus should the first letter of the text be decapitalised, such that:

Input

the OECD has developed an Observatory of Public Sector Innovation (OPSI) which collects and analyses examples and shared experiences of public sector innovation to provide practical advice to countries on how to make innovations work. The OPSI provides a place for sharing, discussing and co-creating solutions that work

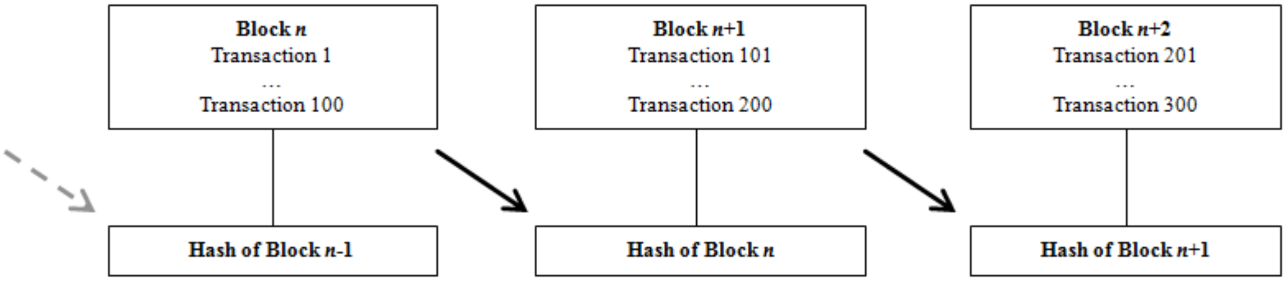
It follows that, once processed, the output is rather different. In this particular case, we find:

Hash

1705df4533240034bd8dda3be4c46081c543250c10ef955ed278c2833af2fa9a

For the sake of clarity, below is the former hash again. Note that there can be no logical relationship between the former and the new hash:

9bb11726ad25d7deb9fe1bcebca51550d19c7cb80d2170a7ca6e8e95f18e5763

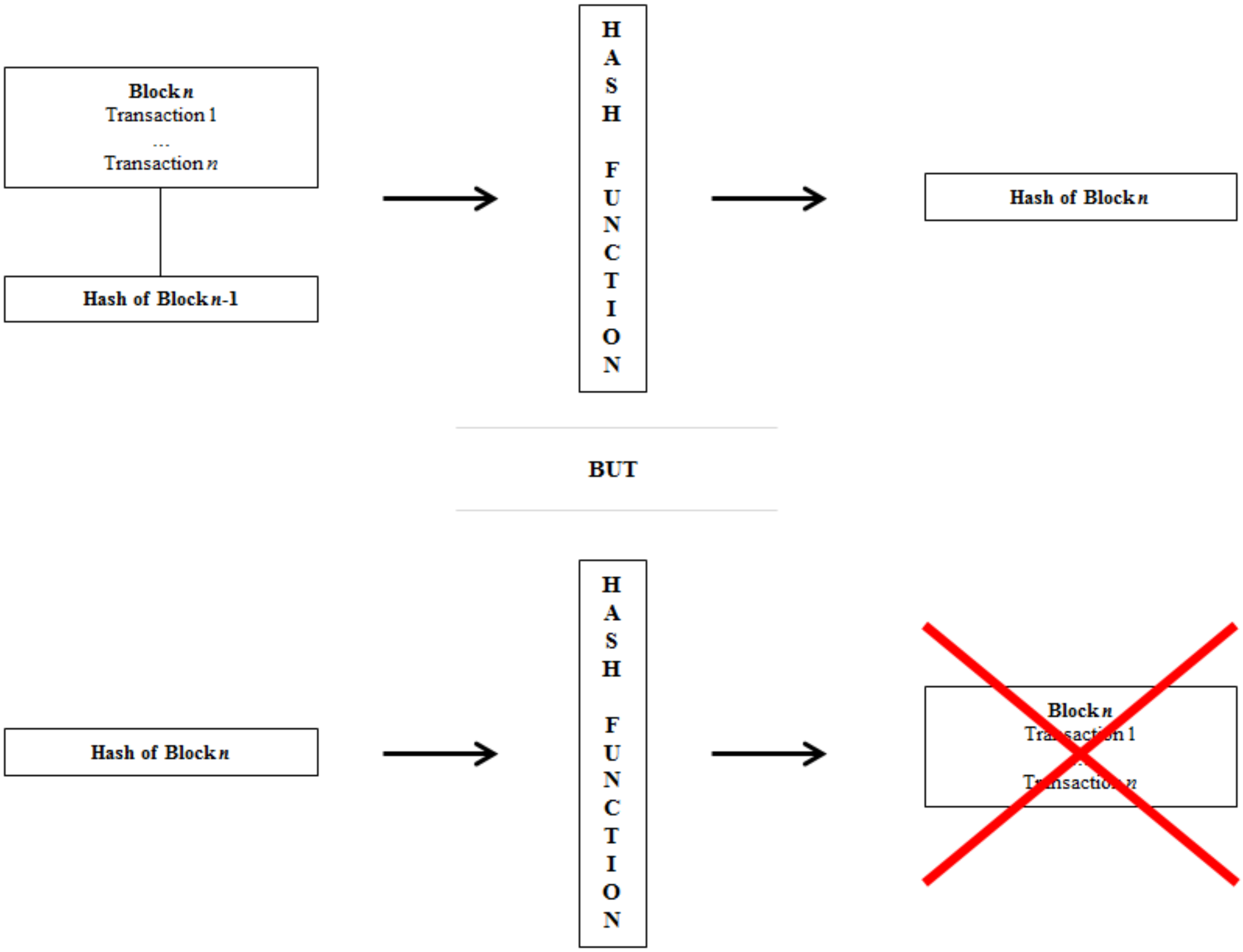


This concept becomes particularly important as it is used to secure a set of transactions into blocks. A given set of transactions, when hashed, provide a hash that acts as a unique digital padlock – thus creating a safe block. To increase security levels, the Blockchain infrastructure adds a layer of complexity: the hash of any block is the sum of the hash of the content of the block *and* the hash of the previous block[4].

Hashing – The interdependence of blocks (David, forthcoming, p.8)

Any aim to tamper with a transaction in *Block n* will ultimately modify the *Hash of Block n*. Logically, the *Hash of Block n+1*, which is the sum of *Block n+1* and the *Hash of Block n+1*, will also change – and so on and so forth. It follows that once the hash of Block *n* is associated to the Block *n*+1, Block *n* becomes ultimately immutable – and its content with it. Else it would imply that the entire chain changes accordingly at a faster pace than it takes to create the subsequent block, which is practically impossible to do.

It is also important to note that hashing is only a one-way process: in other words, while the input provides its own unique hash – in fractions of a second –, the hash *does not* provide the input it has essentially compressed. The cryptographic hash only works as a padlock, but at no point does it play the role of a key. It ensures that the mere possession of the valid hash does not open the way to accessing the block and potentially changing its content.



Hashing – From the input to the hash

The hash is the proof that something indeed *occurred* – that a block was successfully created. Moreover, remember that each node holds identical ledgers – thus it must hold identical hashes for each block of transactions, too. The hash acts as a proof of consensus:

If all nodes produce the same identical hash given an identical hash function, it follows that they had identical inputs to start with. This tests and confirms that there is perfect and identical information on the Blockchain.

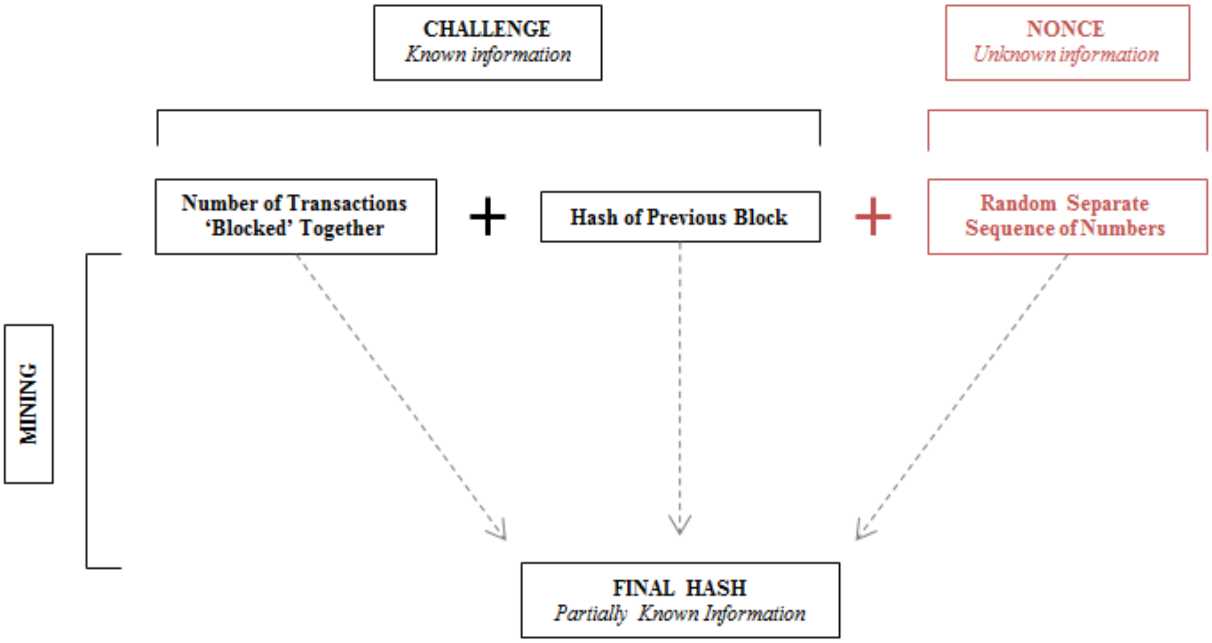
Creating the hash is an essential feature of many Blockchain platforms. It is introduced in Appendix C.

Appendix C: Mining

To best understand the mining process, it is important to take a step back, and dive again into the different steps of a Blockchain transaction:

1. Two parties wish to carry out a transaction, and broadcast their demand onto the entire network;
2. Nodes check their ledgers to ensure that the transaction is feasible and confirm the transaction
3. Once a certain number of transactions have occurred, they must be safely secured within blocks – this is where mining comes into play.

Miners – i.e. powerful computers – aim to find the safest hash / padlock possible. In order to do so – and for a set hash function, as determined by the platform at hand – it takes a set number of transactions that will be 'blocked' together as well as the hash of the previous block – which has been shared on the distributed network hence is known by all nodes. The sum of these two variables is called a *challenge* and, put together, form an input of their own. As we know from hashing – see Appendix B – such input, if compressed by the hash function, would provide a unique output: a hash.


CHALLENGE
Known information
NONCE
Unknown information
Number of Transactions 'Blocked' Together
+
Hash of Previous Block
+
Random Separate Sequence of Numbers
MINING
FINAL HASH
Partially Known Information

The mining process on the Blockchain

Platforms such as *Bitcoin*[5] take security a step further and require another separate sequence of numbers, a *nonce*, to be added to the challenge. This nonce takes the form of a random sequence of numbers that, when added to the challenge, will logically provide a new unique hash. Most importantly, *Bitcoin* requires miners to produce a final hash with one specific characteristic: it must have a set number of zeros in its prefix, such as:

00000000007fc18bc577e227ec7d65a3ced26546bdb2466529ae6149f5d946d2

It follows that the probability of finding the correct hash diminishes as the number of zeros increases, for a fixed hash function and thus a hash of a fixed size.

With a known challenge, it is the role of miners to find the right nonce such that it fits the hash requirements. This can only be achieved through a trial-and-error mechanism: miners 'simply' try an immense number of combinations until the right fit is found. Such process requires computers to try a high number of potential nonces every second and uses up incredibly large amounts of energy.

Once the correct hash is found by a miner, it is automatically broadcasted to the entire network, and all nodes – with identical information – try the nonce for themselves. This is important: while producing the correct hash from a set hash function and input is complex, verifying the validity of this very hash can be done very quickly – and requires little energy. Once confirmed, the block of transaction is finally sealed, and miners go on to seal other blocks of new transactions. This entire process is called a *proof-of-work*: it is the process of proving that the mined hash is indeed valid in light of the three main constraints:

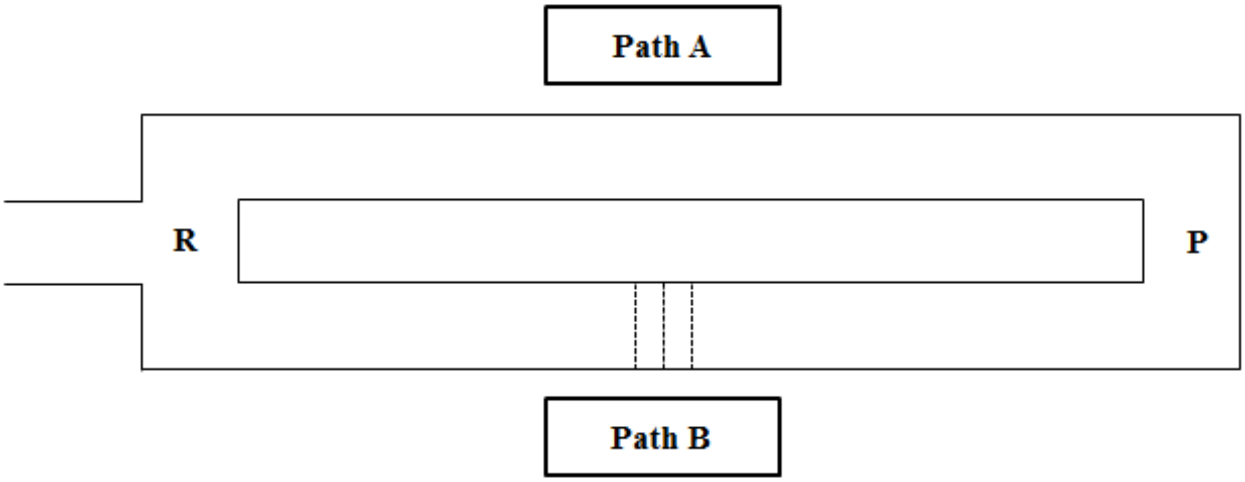
- A set input, in the form of a list of transactions. This is identical among ledgers;
- A set hash function, predefined by the platform once performs transactions on;
- Known hash requirements, also defined by the platform.

This process allows for high levels of security on the Blockchain and thus ensures the immutability of transaction information. Furthermore, the 'winning' miner – the first miner to find the correct proof and broadcast it to the distributed network – receives a set amount of Bitcoins[6]. This creates an incentive for the mining process to keep on going, thus by essence securing the network by even larger extents. This amounts to a powerful self-reinforcing securisation protocol.

Appendix D: The zero-knowledge proof

The Zero-Knowledge Proof is a mathematical construction that responds to the following set of issues:

1. One party (the prover) must prove to another party (the receiver) that a transaction is valid and has occurred;
2. The receiver is *not able* to see the transaction;
3. The receiver must believe without the shadow of a doubt that the prover is saying the truth;
4. There must be no central authority holding any certification role.



This rather counter-productive idea of proving something by the mere act of stating that it is true is better understood with the common analogy of the cave (see Guillou *et al*, 1998). *The Prover (P)* claims that she holds a secret password to open a door that stands in the way of Path B (represented by three dotted lines). However, she is at no point allowed to give the password to the second party, *the Receiver (R)*. A way must be found for *P* to prove that she holds the password, and can take any of the two paths to go around the cave and reach safely to *R*.

Zero-Knowledge Proofs – The Cave Analogy

In order to do so, *P* enters the cave using either path and stands opposite to *R*. *R does not see* which path *P* takes upon entering the cave. Once both are set, *R* calls on *P* to randomly take either of the two paths to return. If *P* says the truth and holds the password, it follows that she can walk back on either of the desired paths. However if she lies and can only return through path A, then *P* only has a 50% chance of returning – that is, there is only a 50% chance that *R* calls Path A. Should this process repeat a large number of times, the likelihood that Path A only is chosen becomes radically small[7]. If *P* continues to return safely to *R* at all times, it logically follows that there is an extremely high probability that *P does* hold the secret password.

Zero-knowledge proofs come down to setting a binary probability with one of the options conditioned on the transaction being valid and having taken place. As the number of tests increases, the probability that the prover lies becomes so extremely small that the transaction can indeed be safely trusted with a high degree of confidence.

References

Interviews

- Herman, Justin, 16 August 2017
- Lemaire, Axelle, 11 August 2017
- Noah, Emmanuel, 2 August 2017
- Raford, Noah, 21 August 2017
- Rinearson, Tess, 6 September 2017
- Segendorf, Björn, 8 August 2017
- Tillemann, Tomicah, 29 August 2017
- Mats Snäll, 24 August 2017
- Yong, Stanley, 10 August 2017

Bibliography

1. Atzori, Marcella, 2015, "Blockchain Technology and Decentralised Governance: Is the State Still Necessary?", *SSRN e-Library*, Online, last accessed 30 August 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

1. Baran, Paul, 1964, "On Distributed Communications: Introduction to Distributed Communications Networks", *United States Air Force Project Rand*, pp.1-2

1. Barr, Dan; Fedesova, Kate; Filipova, Mariya; Housman, Dan; Israel, Adam; Killmeyer, Jason, Krawiec, RJ, Nesbitt, Allen; Quarre, Florian; Tsai, Lindsay; White, Mark, 2016, "Blockchain: Opportunities for Healthcare", *Deloitte*

1. Brandon, Guy, 2017, "Can the Blockchain Scale?", *Due*, Online, last accessed 30 August 2017, https://due.com/blog/can-the-blockchain-scale/

1. "Bitcoin Energy Consumption Index", 2017, *Digiconomist,* Online, last accessed 30 August 2017, https://digiconomist.net/bitcoin-energy-consumption

1. "Bitcoins in circulation", 2017, *Bitcoin.info*, Online, last accessed 24 August 2017, https://blockchain.info/charts/total-bitcoins?timespan=all

1. Buterin, Vitalik, 2015, "Visions, Part 1: The Value of Blockchain Technology", *Ethereum Blog*, Online, last accessed 23 August 2017, https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

1. Cheng, Steve; Daub, Matthias; Domeyer, Axel; Lundqvist, Martin, 2017, "Using Blockchain to Improve Data Management in the Public Sector", *Digital McKinsey*, McKinsey & Company, Online, last accessed 25 August 2017, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

1. Dalal, Darshini; Yong, Stanley; and Lewis, Antony, 2017, "The Future is here – Project Ubin: SGD on Distributed Ledger", *Monetary Authority of Singapore & Deloitte*

1. David, Torben, forthcoming, "Distributed Ledger Technology: Leveraging the Blockchain for ESA", *European Space Agency*

1. Deane-Johns, Simon & McLean Sue, 2016, "Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?", *Morrison & Foerster LLP*, pp.1-8

1. De Filippi, Primavera (2017), "The Interplay Between Decentralisation and Privacy: the case of Blockchain technologies", *Journal of Peer Production, Alternative Internets* 7

1. Deshpande, Advait; Gunashekar, Salil; Lepetit, Louise; Stewart, Katherine (2016), *Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospect for Standards*

1. "Emerging Citizen Technology", 2017, *General Services Administration*, Online, last accessed 24 August 2017, https://www.gsa.gov/portal/category/101958

1. Farell, Ryan, 2015, "An Analysis of the Cryptocurrency Industry", *Wharton Research Scholars*, 130

1. Gabison, Garry, 2016, "Policy Considerations for the Blockchain Technology Public and Private Applications", *Bepress*, European Commission

1. "Global Blockchain Council", 2017, *Dubai Future Foundation*, Online, last accessed 24 August 2017, http://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/

1. Guillou, Louis & Quisquater, Jean-Jacques, 1998, "How to Explain Zero-Knowledge Protocols to Your Children", *Advances in Crytpology – CRYPTO 1989: Proceedings*, vol. 435, pp.628-631

1. Hanson RT, Reeson A, Staples M, 2017, "Distributed Ledgers: Scenairos for the Australian Economy Over the Coming Decades", *Commonwealth Scientific and Industrial Research Organisation*, Camberra

1. Hartung, Adam, 2017, "A Bitcoin Is Worth $4,000—Why You Probably Should Not Own One", *Forbes Online*, Online, last accessed 23 August 2017,

https://www.forbes.com/sites/adamhartung/2017/08/15/a-bitcoin-is-worth-4000-why-you-probably-should-not-own-one/#2b8dc5843b08

1. Kasireddy, Preethi, 2017, "Blockchains don't scale. Not today, at least. But there's hope", *Medium*, Online, last accessed 30 August 2017, https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a
2. "Is Blockchain technology the new internet? A step-by-step guide for beginners", n.d., Online, last accessed 23 August 2017, https://blockgeeks.com/guides/what-is-blockchain-technology/

1. Mamoria, Mohit, 2017, "The ultimate 3500-word guide in plain English to understand Blockchain", *LinkedIn blog*, Online, last accessed 23 August 2017, https://www.linkedin.com/pulse/blockchain-absolute-beginners-mohit-mamoria

1. Marshall, Johnathon, 2017, "Estonia Prescribes Blockchain for Helathcare Data Security", *PWC blog*, Online, last accessed 23 August 2017, http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html

1. Nakamoto, Satoshi, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System", *www.bitcoin.org*, Online, last accessed 25 July 2017, https://bitcoin.org/bitcoin.pdf

1. Nathan, Oz; Pentland, Alex; Zyskind, Guy, 2015, "Decentralising Privacy: Using Blockchain to Protect Personal Data", *IEEE Security and Privacy Workshops*

1. OECD, 2016, "OECD Science, Technology and Innovation Outlook 2016", *OECD Publishing*, Paris

1. OECD, 2017, "Embracing Innovation in Government: Global Trends", *OECD Publishing*, Paris

1. Ølnes, Svein, 2015, "Beyond Bitcoin – Public Sector Innovation Using the Bitcoin Blockchain Technology", *International Conference on Electronic Government and the Information Systems Perspective*, Springer, pp.253-264

1. "Ordonnance n.2016-520 du 28 avril 2016 relative aux bons de caisse", 2016, *Journal Officiel, 29 avril 2016, texte n.16*

1. Patrick, Gabrielle, 2016, "Europe's Regulatory Blockchain Shift on Display at Private Parliament Event", *CoinDesk*, Online, last accessed 23 August 2017, https://www.coindesk.com/the-eu-regulatory-blockchain-shift/

1. "Police Need Power to Tackle Virtual Money Laundering: Europol", 2014, *Reuters*, Online, last accessed 30 August 2017, http://www.reuters.com/article/us-bitcoin-europol-money-laundering-

idUSBREA2N1A420140324

1. Rinearson, Tess, 2017a, "Making Money: Bitcoin Explained (with Emoji), Part 1", *Medium*, Online, last accessed 23 August 2017, https://medium.com/@tessr/making-money-530d2bb2b8f7

1. Rinearson, Tess, 2017b, 'Making Money Trustworthy: Bitcoin Explained (with Emoji), Part 2", *Medium*, Online, last accessed 23 August 2017, https://medium.com/@tessr/making-money-trustworthy-6c552a1cfc25
2. Rosenfeld, E. and E. Cheng (2017), "Bitcoin sees sudden, sharp spike after smashing through $10,000", CNBC, 29 November 2017, www.cnbc.com/2017/11/29/bitcoin-sees-sudden-sharpspike-after-smashing-through-10000.html.

1. Snäll, Mats, "Blockchain and the Land Register – A New 'Trust Machine'?", n.d., Submission n.572

1. Stawinska, Karolina, 2017, "Meet 10 Millenia Entrepreneurs Who Are Rethinking Industries", *Medium*, Online, last accessed 24 August 2017, https://medium.com/swlh/meet-10-millennial-entrepreneurs-who-are-rethinking-industries-5f064cd37343

1. "The promise of the Blockchain: The trust machine", 2015, *The Economist*, Online, last accessed 23 August 2017, https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

1. "The Social Smart Contract: An Open Source White Paper", 2017, *Democracy Earth Foundation*, Online, last accessed 31 August 2017, file:///C:/Users/Bourgery_T/Downloads/The%20Social%20Smart%20Contract.pdf

1. Walport, Mark, 2016, "Distributed Ledger Technology: Beyond Block chain. A Report by the UK Government Chief Scientific Advisor", *UK Government*

1. Webb, Steve, 2016, "Why Central Banks Are Getting Serious About Blockchain", *Medium*, Online, last accessed 25 August 2017, https://medium.com/@InnFin/why-central-banks-are-getting-serious-about-blockchain-19b695095e98

1. Willms, Jessis, 2016, "Is Blockchain-Powered Copyright Protection Possible?", *Bitcoin Magazine*, Online, last accessed 30 August 2017, https://bitcoinmagazine.com/articles/is-blockchain-powered-copyright-protection-possible-1470758430/
2. Willms, Jessis, 2016, "Is Blockchain-Powered Copyright Protection Possible?", *Bitcoin Magazine*, Online, last accessed 30 August 2017, https://bitcoinmagazine.com/articles/is-blockchain-powered-copyright-protection-possible-1470758430/
3. Yaga, Dylan; Mell, Peter; Roby, Nik; and Scarfone, Karen, 2018, "Blockchain Technology Overview",

United States National Institute of Standards and Technology (NIST),
https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

[1] Though this is more geared towards the private sector and the developer's community ↑

[2] This next section is inspired from Rinearson, 2017b ↑

[3] Given one same hash function – see Faife, 2017 for a detailed and technical explanation ↑

[4] In some platforms, the hashing process is even more complex, for greater security levels. This protocol, known as *Proof-of-Work*, is presented in Appendix C ↑

[5] Things are different on *Ethereum* – see Kasireddy, 2017 ↑

[6] At the time of this report, it amounts to 25 BTC ↑

[7] The probability that R always calls Path A is equal to 0.5^n, where n is the total number of reiterations ↑