Distributed Ledger Technology & Cybersecurity

Improving information security in the financial sector

DECEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Dr. W Kuan Hon, kuan0.com

John Palfreyman, Director - Blockchain, National Security IBM Cloud Division, Europe CTO Team

Matthew Tegart, ING Direct, Australia

978-92-9204-200-4, 10.2824/80997

Table of Contents

1. Executive summary

Distributed ledger technology – commonly referred as Blockchain – has emerged as candidate for financial institutions to reform their businesses. The speed and cost of doing business using distributed ledger technology is expected to improve by simplifying back-office operations and lowering the need for human intervention. However, a number of security concerns around this new technology remains.

Instead of depending on a central entity such as a single financial institution to track the validity of ownership of funds, a distributed ledger maintains all transactions and holdings and is updated by a number of counterparties.

The distributed ledger allows counterparties to use smart contracts[1] and enhanced transaction privacy. Updates to the Blockchain or "distributed ledger" leave an audit trail and allow auditing to verify how an agreement was executed. Blockchain protocols are believed to provide a transaction and application environment, by using a mix of consensus and transaction protocols to determine valid transactions, as well as reach agreement on the current state of items such as a contract or account balance.

This paper aims to provide financial professionals in both business and technology roles with an assessment of the various benefits and challenges that their institutions may encounter when implementing a distributed ledger. Some of the key challenges of Blockchain identified in the document are:

- **Traditional challenges** such as:
  - Key Management
  - Privacy
  - Code Review
- **Technology specific challenges** such as:
  - Key Generation
  - Smart Contract Management
  - Scalability

ENISA has also identified good practices to overcome the issues identified as well as introduce the key concepts that decision-makers should be aware of when approaching this technology. After reviewing the existing challenges attached to distributed ledgers, some good practices are:

- Using recovery keys
- Using multiple signatures for authorizing and processing transactions
- Using library of standardized smart contracts

[1] Szabo, Nick. "The idea of smart contracts, 1 997." (1997).

In this paper, we have also identified that there are challenges that may require further development, such as:

- Anti-money and anti-fraud tools
- Interoperability of Blockchain protocols
- Legal provisions and tools for implementing privacy and the right to be forgotten

Throughout this paper, we refer to the words Blockchain and distributed ledger interchangeably. Although they do not always share the exact same underlying technical mechanisms, these technologies often follow the same principles of allowing counterparties to exchange data and automate contractual obligations.

2. Drivers of adoption for Financial Institutions (FI)

As financial services move towards digitisation, financial institutions will need to operate lower cost, high volume payment lines to service their retail business, whilst catering to the increasing demand for security and mobility. There are also increasing demands for efficiency and transparency from institutional counterparties and financial services regulators, on business and technology processes.

The main drivers behind the adoption of distributed ledger technology are:

- **Cost reductions -** The opportunity for financial institutions to unplug legacy systems and reduce the amount of layers required for data sharing. By ensuring data is natively in digital format and shared at the point of transaction, reconciliation time can also be drastically reduced.
- **Risk-management -** The ability to predict and avoid overextending an institution's liabilities. By providing a standardised framework for recording even complex transactions such as derivatives, financial institutions can make it much easier to manage their risks and positions in real time.
- **Regulatory compliance** - compliance with the requirements of various sets of legislation, as well as conducting only authorised transactions can be automated to a great degree.

Financial institutions currently operate their own database silos, which are then reconciled against each other to ensure data is valid. Blockchain technology can provide a single distributed ledger of transactions and messages.

To operate effectively, the financial system requires its actors to fulfil their engagements and comply with existing legal statutes as well as operate in a structured fashion. This is achieved by a combination of means, which we refer to as a "governance toolkit":

- **Regulation** - An authorisation body is appointed, which can designate individuals and firms as authorised to transact within specific markets. In the wake of the global financial crisis of 2008 and the resulting increase in regulatory requirements, the additional costs of meeting regulatory compliance and auditing requirements is evaluated at up to $4Bn yearly[2] for some banks.
- **Audit** - The financial institution must make certain business information available to the regulator on a regular basis, to prove their compliance with specific rules.
- **Internal Controls** - A financial institution will monitor its' various business lines using a range of risk-management metrics to keep business activity in line with capital and risk requirements. Additionally, managerial and organisational processes are used to maintain human agent behaviour within acceptable parameters.
- **Technology** - At any one time, large financial institutions have a number of technology related projects under development which allow them to transact, report on data or interface with counterparties. Current technological implementations suffer from having to integrate with previous systems, resulting in a patchwork of legacy technologies that require ongoing maintenance.

The above tools, applied collectively, allow financial institutions to comply with regulatory requirements, send transaction messages to counterparties and reconcile data. However, recent years have shown the extent to which these tools can be insufficient. The "governance toolkit" is vulnerable to either dishonest human activity, data entry mistakes, or technological shortcomings.

[2] Accenture, *Investment Banking Technology: Jettisoning legacy architectures*, 2015 (link – last accessed August 2016)

Distributed ledger technologies might allow institutions to embed their operating rules within code. From a governance perspective, this means that the business functions of regulation, audit and internal controls can be embedded into the transaction system. For example:

- **Regulation changes**
  Distributed ledger technology could assist the financial institutions and regulators in a way that once a new regulation is coded into the distributed ledger it is spread to all, without any need of technical change required from the counterparties.
- **Audits**
  Audits mainly show a status of a given system or organization in a given point in time- distributed ledger technology could potentially allow for **continuous monitoring**.
- **Business logic**
  At the scale of an individual financial institution, **business logic can be programmed into smart contracts, drastically simplifying back-office operations**, especially with regards to data reconciliation and asset or funds settlement. By establishing a common protocol for transaction and settlements, financial institutions can move towards near real-time settlement.
  - If all financial transactions are recorded on regulated ledgers, it might be possible to implement prudential regulations. For example, this could automatically restrict new transactions that cause an institution's balance sheet to exceed risk-management parameters issued by the regulators to whose jurisdiction the financial institutions are subject.
- **Reduce the need for internal monitoring**
  With the support of Blockchain transactions that will now be conducted and settled by software rather than staff. The requirement for regular data audits will remain, to ensure that the smart contract has been executed as intended.
- **Achieve consensus in an uncertain environment**
  The nature of the distributed ledger allows for reaching consensus over a certain transaction even when you may not trust the counterparties in the network.

Blockchain technology must not be seen as a replacement to financial institutions for the operation of the financial system. It is a technological tool, which can be used by parties such as major financial institutions and regulators to share information and transact more easily whilst maintaining control over their information.

3. Distributed Ledger Technologies

Here we show key components and properties which we think are important and valuable for the financial institutions.

Usually, the distributed ledger has the following model (see Figure 1):

- All participants share a consistent copy of the database, there is no central server
  - Some participants might not have a full copy
- Network connections are peer-to-peer
- Participants must comply with ledger rules
  - **permissionless ledger** – anyone could join
  - **permissioned ledger** – participation is subject to rules of the members
- Using a type of **consensus protocol,** to agree on validity of a given transaction
- **Transactions** – could be financial and/or exchanging of assets and/or services
  - Rules for a transaction could be coded into what is called **smart contracts**
- **Uses digital signatures (private/public key)** to sign and/or encrypt transactions on the ledger
  - Signatures could be linked to identity
- Represents a temporal order of how assets evolve over time

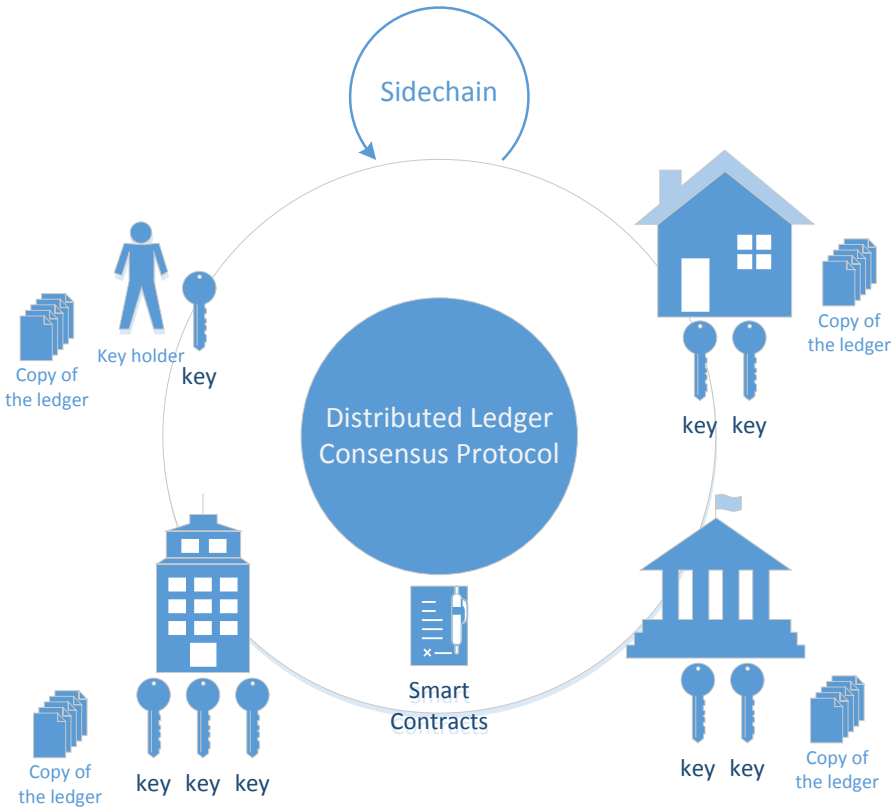


Figure 1: Distributed Ledger Ecosystem

3.1 Miner

A miner is a participant in a Blockchain that participates in securing the network and validating new transactions. The mining and validation process happens via either competitive, voting or luck-based methods dependant on the consensus protocol chosen. Miners are incentivised to participate in a Blockchain either because they receive mining rewards in the form of cryptocurrency (eg. Bitcoin) or because they have a vested interest in accessing and exchanging data on that network (such as a business that chooses to participate in an industry or market-specific Blockchain).

3.2 Consensus protocol

The core difference between a distributed ledger and a traditional database is the way in which datasets evolve over time. The system allows multiple participants to submit new inputs to a distributed ledger. Consensus is then used to determine over time which state of the database is considered as valid. This is in contrast to a traditional database, where multiple participants submit new inputs and one counterparty is relied on to provide the valid state of the database.

Consensus protocols are the mechanisms by which all users within a distributed ledger agree on the validity of the underlying data.

One of the key aspects of a distributed ledger is that the data held within it, is considered valid because all parties agree to a single "true" version. In the event that existing participants in a Blockchain decide to include data in a non-compliant manner with established protocols, an event named a fork occurs.

Forks result in a split of the ledger and the consequent creation of two groups, each validating their own version of the ledger. In order for participants to be able to continue to interact with each other, they are required to follow the same fork of the ledger.[3]

The following table gives a brief overview of main consensus protocols in use:

CONSENSUS PROTOCOL	OVERVIEW
Proof of Work	Uses computational power to validate new blocks of data. To participate in this scheme, participants are required to collate transactions within a single block and then apply a hash function with the use of some additional metadata.
Proof of Stake	Validators (special nodes) voting on valid blocks whilst posting collateral in order to be able to participate in the validation process. Unlike Proof of Work, Proof of Stake relies on proving the user is invested in the underlying token of value of the network being mined rather than being the owner of a large amount of computing power
Ripple Protocol	In order to validate new transactions, servers amalgamate outstanding transactions into a "candidate list." All participants then vote on valid transactions to be included in the ledger.

[3] A case study of a fork can be found in Annex B of this document

	Transactions that meet the 80% threshold of "yes" votes are included within the following last closed ledger state.
Proof of Elapsed Time	As part of its Intelledger proposal, Intel has devised a means of establishing a validation lottery that takes advantage of the capability of its CPUs to produce a timestamp cryptographically signed by the hardware. Whoever in the chain has the next soonest timestamp will be the one to decide which transactions will be a part of the next block in the chain. This consensus method is extremely energy efficient compared to Proof of Work and therefore more adapted to IoT devices.

Table 1: Consensus protocols

3.3 Cryptography

Distributed ledger technology relies on the use of asymmetric cryptography to sign messages and encrypt data through the use of a private/public key pair. Key sizes depend on the implementation of the ledger and could vary.
Cryptography is also involved in some of the consensus protocols (e.g. Proof of Work) and is the primary vehicle in achieving consensus.

The private keys, which allow a given entity to transact with the assets or virtual currency allocated to it in the Blockchain are typically stored in what is called a wallet. In a given wallet, there could be multiple keys stored.

3.4 Sidechains

The standard operation of a distributed ledger might allow thousands of transactions which in some cases, might result in slow processing. In an attempt to resolve this problem, one technology that has been developed is the concept of side chains.

- These are the concept of running a separate distributed ledger off of the main chain but with transactions able to take place in the same currency as the core system
- By performing transactions on a such specialized ledger, transactions should be processed faster
- Users who are able to see the content of a transaction, may also be restricted depending on that sidechain's implementation

Another sidechain[4] proposal establishes the idea of pegged sidechains**.** Pegged sidechains would enable digital virtual currencies and/or other ledger assets to be transferred between multiple Blockchains.

3.5 Smart Contracts

Business activities require counterparties to trust each other, and ensure they share the same understanding of transaction details. Contractual obligations carry three key characteristics, as outlined by researcher Nick Szabo[5].

- **Observability**
  The ability of the principals (parties to the contract) to observe each other's performance of the contract, or to prove their performance to other principals.

[4] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, P. Wuille, *Enabling Blockchain Innovations with Pegged Sidechains*, 22nd October 2014
[5] Nick Szabo, *Formalizing and securing relationships on public networks*, First Monday Vol. 2 Number 9 September 1997

- **Verifiability**
  The ability of a participant in a contractual agreement to prove to an arbitrator that a contract has been performed or breached, or the ability of the adjudicator to find this out by other means.
- **Privity**
  The principle that knowledge and control over the contents and performance of a contract should be distributed among parties only as much as is necessary for the performance of that contract. A generalization of the common law principle of contract privity, which states that third parties – other than the designated adjudicators and designated intermediaries – should have no say in the enforcement of a contract.

Blockchain-based applications involve the use of smart contracts, a direct application of Szabo's principles.

Smart Contracts

"Contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system."[6]
Smart contracts allow participants to verify that counterparties have fulfilled their obligations and provide for an accelerated, automated, settlement once the required conditions have been met (such as a payment or asset transfer).

3.6 Permissionless Ledgers

A permissionless ledger is defined as a Blockchain protocol where a client may operate a full node without prior approval (i.e. download a copy of the database and act as a validator for future transactions). The advantage of a permissionless ledger is that, as it gains adoption, it becomes highly decentralised and redundant, becoming very difficult to shut down.

Furthermore, applications deployed within a permissionless ledger will be able to natively interact with other applications on the same ledger. If two applications are on separate ledgers, then a communication channel becomes required.

3.7 Permissioned Ledgers

Permissioned ledgers are a form of distributed ledger that operate as a "members' club". In this environment, the underlying consensus protocol is freely chosen by the group that initiates the protocol.

In the example of a group of financial institutions:

- they would agree on a common distributed ledger protocol
- Consensus protocols changes could potentially happen if adopted by all the counterparties
- Its' members will be able to vet and add new counterparties, as well as remove existing ones.

Though financial institutions may use permissionless chains to hash some private data as well as trade on specific public, open, markets, the largest likelihood is that most applications and financial systems will be implemented as permissioned ledgers, managed by a quorum of counterparties. A permissioned ledger could allow financial institutions to leverage their real-world reputation. In this case, the FI will not want to perform malicious actions on the network, as this will damage their brand.

[6] UK Government Office for Science, p.18, *Distributed Ledger Technology: beyond blockchain, 2016*

As outlined, distributed ledger technology offers a novel set of solutions to enable entities to transact with others in a safer environment. However, the extent to which this is a security improvement will now be the focus of our next section.

4. Cybersecurity Challenges

In this section we aim to identify the challenges associated with the distributed ledger technology. As this technology is in its development stage the challenges recognized should not be considered as complete list of challenges.

4.1 The Traditional Challenges

The use of a distributed ledger implies that data is shared between all counterparties on the network. On one side this could potentially have a negative impact on the confidentiality; while on the other, it has a positive impact on availability with many nodes participating in the Blockchain, making it more robust and resilient.

4.1.1 Key Management

Private keys are the direct means of authorizing activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys.

The methodology of the attacks seeking to gain unauthorised access to a system via stolen credentials remains fundamentally the same- try to capture information, plant malware and/or use social engineering to steal the private keys from the user's machine.

Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a dataset would be able to read the underlying data. However, if the signing key is secured, they will not be able to modify the data or interact with that smart contract (providing it has been appropriately designed).

The significance of protecting the private key is due to the fact that actions taking place on a hacker's machine, such as file decryption attempts or private key reproduction, are not subject to server imposed query limits and are run without anyone else being able to notice.

Unlike with traditional systems, where before a server administrator was capable of tracking attempts to break into a customer or user account, the malicious users can keep trying limitlessly to decrypt or try to reproduce a private key out of encrypted data from a given ledger. With Blockchain, there is no way of knowing this is happening until after the hacker has succeeded.

4.1.2 Cryptography

Most Blockchain implementations rely on the cryptographically generated public and private keys to operate.

Main challenge associated with cryptography is that stringent policies and procedures must be followed when managing keys, including people, processes and technology.

Usually, the user generates the private and public keys using software, such as the Blockchain client software, or another available software. It has already been shown, that some programs are generating keys that have been identified to be weak[7]. There are also documented[8] attempts to spread intentionally

[7] Coindesk, *Open-Source Tool Identifies Weak Bitcoin Wallet Signatures*, October 16th 2014
[8] N. Heninger, *How not to generate random numbers*, May 13th 2015, University of Pennsylvania

weakened random number generators, from which a limited range of possible values can be produced. Keys generated through these limited random number generators could be more easily brute forced.

Quantum computing may also threaten the premise of asymmetric cryptography. Though it does not represent an immediate threat, it should be certainly taken into consideration for a future-proof solution. Popular security algorithms that are used for securing information through a complicated challenge (e.g. RSA, ElGamal), may now be resolved in a shorter amounts of time through the use of quantum computing.

4.1.3 Privacy

Privacy is an additional issue that emerges from the use of Blockchain technology.

In a permissionless ledger, all counterparties are able to download the ledger, which implies that they might be able to explore the entire history of transactions, including those to which they were not members of. The "right to be forgotten" where information needs to be removed from a ledger is challenging to implement. Usually, many counterparties have the data from the ledger, and it would be difficult to prove that all data has been deleted.

The solution of Hyperledger for example, offers to solve this by offering a range of commercial privacy services.

Additionally, there is a challenge with smart contracts being able to access the data in order to process transactions. Since this is possible, there is possibility that a smart contract might be able to leak information on what is being processed. In this way, privacy might be breached.

4.1.4 Code review

Whilst many skilled eyes may have reviewed the protocols, methods, and codebase of popular implementations of distributed ledgers, it remains possible that unknown vulnerabilities exist.

4.2 The Distributed Ledger Specific Challenges

In addition to the traditional security concerns, Blockchain brings additional security challenges and attack vectors. Some of these are unique to specific implementations, and others exist across all designs.

4.2.1 Consensus hijack

In decentralized, permissionless networks, where consensus is formed through majority, taking control of a large enough portion of participating clients could allow an attacker to tamper the validation process.

In the case of Bitcoin, this is referred to as a "51% attack[9]" where the majority (defined as the proportion of all hashing power in the network) is compromised or controlled by the same entity or a coalition of dishonest counterparties. An attacker would be able to produce new blocks faster than the rest of the network (in proportion to their computing power) leading participants to consider that chain as valid.

The extent of a 51% attack will allow an attacker to refuse to process certain transactions as well as to re-use an asset which has already been spent.

There is possibility, that in a permissionless distributed ledger, the computational power required to hijack the consensus might be cheap enough for a malicious attacker to buy (from a cloud provider for example). This depends on the number of participants and the computational power required for such case. In

[9] I. Eyal, E. Sirer, *Majority is not Enough: Bitcoin Mining is not Vulnerable*, November 1st 2013

situations like this, even one participant might hold the possibility to validate transactions and direct the flow of transactions in the ledger. This is contrary to the notion that, usually, in distributed ledgers one participant doesn't have enough resources to influence the consensus process.[10]

Another consequence of such an attack is in the perspective of adoption. Any chain coming under attack might see an outflow of participants, leading to the question of which chain should be considered as the "main" one to follow as well as potentially crippling the value of that chain.

Another challenge comes from consensus protocols that do not involve some way of penalty to the participants. In this way for a malicious user would be easier to attack.

4.2.2 Sidechains

Whereas major Blockchains like Bitcoin and Ethereum have sufficient adoption to be protected by their mining process against all but the most resourceful attackers, sidechains are more at risk due to their more specialised focus. Where a user has no interest in tracking the data and maintaining the operation of a sidechain, they will not contribute the relevant mining power to secure that chain.

Another vulnerability of sidechains consists in the gateway used to transfer assets and messages between chains. In the case of a Bitcoin sidechain, a user will "lock" Bitcoins in an address on the main Bitcoin Blockchain and then issue proxy tokens for these on the sidechain. If users can also later exchange sidechain tokens for the original token, this mechanism is called a 2-way peg. They can then transact with others on that sidechain. If the initial "locking" transaction is later considered invalid, then subsequent proxy-token transactions would also be affected. Additionally, owners of proxy tokens that had been affected would not be able to convert these back to the original asset via the pegging mechanism.

Fraudulent transactions or attacks on a sidechain do not affect the validity of data held on the parent chain. However, in the event that a sidechain was to be put out of service, the parent chain might be subjected to high stress levels as the sidechain users migrate their transaction volumes to the parent chain.

4.2.3 Exploiting Permissioned Blockchains

In a regulated, permissioned network, where consensus might be implemented under the regulator's direction, any exploitation of the regulator's capabilities would be even more and immediately severe. The extent of the impact depends on the range of capabilities ascribed to the regulator within that specific system.

All problems that had required hijacking of the majority consensus, a task that was a potentially significant in undertaking, are now replaced by the hijacking of a single entity.

The challenges created by the above could be mitigated by implementing a fixed-time notice period prior to regulator-issued major protocol updates being made effective. However, until the intrusion is detected, malicious activity would still be possible within the scope of the regulator's ongoing activities, such as whitelisting individuals or institutions to participate in the system.

[10] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014.

4.2.4 Distributed Denial of Service

Distributed Denial of Service attacks coming out of the nature of the distribute ledger remain a concern. For example, if rogue wallets decide to push large numbers of spam transactions to the network it could create potentially a denial of service and increase the processing time, as the nodes will be checking the validity of the fraudulent transactions.

In March 2016, the Bitcoin network was slowed to a near halt. The cause was a Bitcoin wallet pushing large volumes of spam transactions with a higher than average transaction fee. This caused miners to prioritise these transactions when computing new blocks.

Within a permissioned ledger, it would be possible for nodes to agree to ignore or even block the issuer of such spam transactions. However, if an attacker is able to control a large number of clients, they might be able to severely disrupt the network by pushing large volumes of irrelevant transactions.[11]

The distributed nature of Blockchain architecture introduces the prospect that it would be difficult to shut down a malicious program.

With the capabilities of newer protocols offering data storage and computation, it would be possible to store malicious data within the Blockchain network. Additionally, an attacker could reassign control of the related smart contract at will, leveraging the trustless nature of the Blockchain to buy and sell malware between anonymous cryptographic keys[12].

4.2.5 Wallet Management

Wallet management represents the process and technology used with which a wallet software operates with the keys assigned to it. The wallet software would need to protect the keys from being accessed without authorization, in both cases while stored, but also while in operation with the software.

Losing access to a given wallet might preclude a financial institution from authorising transactions or moving assets. It might be difficult for an entity to be aware that a malicious user has access to the wallet, because copying or stealing the keys might not leave any trace on a computer. By the time an entity understands that the keys are compromised, because of a fraudulent transaction for example, it might be too late for reversal.

4.2.6 Scalability

Removing the need to reconcile counterparty data introduces a scalability problem. On one hand the growth of the ledger size and on the other the speed at which transactions are processed.

The need to store all data pertaining to a specific distributed ledger, may grow to be unmanageable in size for individual end-users.

In the case of a financial market implementation, we assume that major financial institutions act as full nodes. Where the Bitcoin Blockchain has exceeded 90Gb, the Ethereum Blockchain exceeds 10Gb (depending on client used). In terms of keeping a full copy of the database, this doesn't look like a big

---

[11] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401

[12] D. Roffel, C. Garrett, *A novel approach for computer worm control using decentralised data structures*, December 13th 2014

number, but its growth is exponential and has grown for four years around 450% (Bitcoin from July 2012 to July 2016).

The speed at which a given transaction is processed, in some implementations of the ledger, may not be sufficient or acceptable[13].

Exposed to the high transaction volumes of financial institutions, a completely distributed ledger might subject users to performance issues as their machines struggle to maintain an ever growing chain. The transaction speed also depends on the consensus protocol. In the case of Proof of Work consensus protocol the validation of transactions needs to be verified by a number of other nodes which requires processing time. The more participants need to verify a transaction, the more time it will take to be accepted as valid in the ledger. On one hand, participants might not have sufficiently powerful hardware to validate a transaction. On the other, the ledger protocol itself would be designed to accommodate more general requirements, thus bringing more delay. In a consensus protocol that would just use time stamping, the process of validation will be faster compared to the Proof of Work.

The possibility that only specific transactions are to be verified by specific nodes (validators) is called Sharding.[14] Sharding could also introduce a significant fault (ie. reversion of subsequent transactions) if a specific subset of validators were to wrongly validate transactions to which other members of that same Blockchain refer to. This is due to the fact that communication between shards will require the use of transaction receipts from one shard to communicate with the next.

The process of downloading block headers (which are a hashed version of past data) as well as the underlying data for most recent blocks and then cross-reference this with other nodes (rather than downloading the entire database) is called Blockchain pruning. Here, a challenge exists if an attacker were to convince a user that the fraudulent block headers they verify, are genuine.

4.2.7 Smart Contract Management

Smart contract management refers to the people, processes and technology used when creating a smart contract.

Smart contracts are essentially programs that run on the distributed ledger. They are prone to any faults associated with code. As with any software, the more complex a smart contract is, the more prone to software errors it will be.

Generally, the function, and the security of smart contracts code depends on the author's capabilities.

A review by Peter Vessenes[15] found that large numbers of template contracts available on the web for the Ethereum scripting system contained significant vulnerabilities to their operation.

[13] Note: For reference, at the time of writing the Bitcoin transactions are limited to 7(seven) per second, Visa handles at an average of 2000 (two thousand) per second

[14] *V. Buterin, DEVCON1: Scalable Blockchains & Asynchronous Programming, Nov. 9th 2015*

[15] P. Vessenes, *Ethereum Contracts are Going to be Candy for Hackers*, May 18th 2016

On June 2016 an attack on the DAO[16] took place, which was an investment vehicle created on the Ethereum network and operated as a smart contract. Over $59m in Ether[17] were stolen by an unknown source from the wallet controlled by the program on behalf of all investors.

4.2.8 Interoperability

Using different distributed ledgers will very likely bring the need of data sharing between them.

Exchanging data will require translation of formats and protocols, which currently are in very early stages.

Also having to reconcile transactions between different distributed ledger brings another challenge to consider, as different consensus protocols might not be easy to transpose from one to another. Key challenges related to interoperability are:

- Who can transfer assets between distributed ledgers?
- Who can oppose to transferring assets?
- Should transfers allow for whole asset or just part of it?
- Should changes of ownership or asset (theft, loss) be also proliferated to the other chains?

Another interoperability challenge arises from the use of wallet software with different distributed ledgers. Currently, most distributed ledgers come with their own wallet software, and it is difficult to have a common wallet for different distributed ledgers.

4.2.9 Governance controls

Institutions still need their staff to sign off on requests and transactions, though a distributed ledger may transparently indicate which financial institution was involved in a transaction. A challenge becomes how exactly the governance structure could be coded into the distributed ledger.

Another aspect of governance lies at the systemic level, where some institutions may have rules concerning which business activities they can engage in. For example, in the distributed ledger there might be rules for some financial institutions to be allowed to transact with only specific entities, or provide only specific services.

4.2.10 Anti-fraud and Anti-Money Laundering Tools

Another key problem is a lack of tools to combat illegal activity. Though it might be possible to identify who owns an address used for money laundering despite attempts at obfuscating the transaction[18], it is not possible to block these types of transactions in advance. Also, the consensus-based nature of adoption combined with the cross-application and industry aspirations of Blockchain technology means protocols may not evolve sufficiently fast or in correlation with more complex business needs.

The European Commission has already begun researching the foundations of a Public Key Infrastructure, that will impose Anti-Money Laundering (AML) compliance on all entities acting as gateways towards the

[16] See annex B
[17] Zerohedge, *Bitcoin's Largest Competitor Hacked: Over $59 Million "Ethers" Stolen In Ongoing Attack*, June 17th 2016
[18] M. Möser, *Anonymity of Bitcoin Transactions – An Analysis of Mixing Services*, 2013

cryptocurrency ecosystem. Within the financial sector, this could give way to a whitelist of approved public keys whose owners are institutions and professionals who have been allowed to transact.[19]

Another issue that arises with users is that the Blockchain network could be more trustworthy than the machine used to access it. Hence, though the record of the transactions would be verifiable, the intent to perform that transaction might not be. An example of this would consist in the transfer of a large sum of money. Because it happens on a distributed ledger, the transaction is visible and verifiable by all other entities on that ledger. However, the owner of the wallet may not have had the intent of making such a transfer and been subject to a hack. The decentralised chain design also means that it is not possible to simply revert previous actions.

A further potential vulnerability lies not just in the consensus protocol, which exists to provide an accurate historical presentation, but in the transaction protocol used to broadcast messages to the rest of the network. Fraudulent transactions exist in various types:

- **Double-spending:** This involves sending two transactions, one of which will cancel the other. In the example of Bitcoin, until the UTxO set of the Blockchain has been sufficiently confirmed after enough time, counterparties expose themselves to the possibility that the payment received will be invalid.
- **Hacked key:** This type of transaction is broadcast to the network but has not been conducted by the true owner. This happens when a third party obtains unauthorised access to a key.
- **Non-compliant transaction:** This type of transaction is mainly applicable to permissioned, regulated networks. It involves broadcasting a message either from an unauthorised address or against pre-defined business rules. Hyperledger solves this issue with a blend of enrolment (authorisation) certificates and single use transaction certificates to allow transactions.

[19] European Commission, p.7 *Proposal for amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, 2016

5. Good Practices

Having identified key challenges related to Blockchain implementations, our recommendations focus on the good practices to adopt within each category. Some of the good practices are very well documented like the key management, others have been identified during our research. The good practices can be implemented by institutions which wish to participate in a distributed ledger network.

5.1 Key Management

CHALLENGES	GOOD PRACTICES
key storage key loss key theft	• Store keys according to good practices[20] • Use rules that require the use of multiple signatures to authorize and/or create transactions • Allow the use of recovery agents - one way of doing this is through a trusted third party which holds, the keying material required to recover keys • Use different keys to sign and encrypt • Enable internal identification of the individual signing off the request for a transaction • Issue individual keys to persons working on behalf of institution

5.2 Cryptography

CHALLENGES	GOOD PRACTICES
Key generation	• Make sure the keys are generated in a secure and valid way[20] • Make sure the key length is appropriate for the use[20] • Use different keys to sign and encrypt

5.3 Privacy

CHALLENGES	GOOD PRACTICES
Keep information visible only to authorized entities Unauthorized access to transactions	• Encrypt the transactions, so only the involved counterparties can access the whole information • Use sharding to allow specific transactions to be validated by specific entities • Use pruning to remove data from the ledger at certain period of time, as requested by the regulation • In case an entity must be linked to a key, an authority may keep information of which key belongs to which entity • Encrypt ledger with more than one key

5.4 Code review

CHALLENGES	GOOD PRACTICES

[20] Smart, N., et al. "Algorithms, key size and parameters report.", ENISA (2014).

Bugs/Errors Zero-day attacks	• The institutions offering Blockchain applications should ○ do code review (or employ third party services) of Blockchain applications and associated libraries ○ Apply Software Development Life Cycle principles ○ Do penetration testing (or employ third party services) of the Blockchain application

5.5 Consensus Hijack

CHALLENGES	GOOD PRACTICES
Fraudulent transactions	• Monitor if one of the nodes increases processing power and is executing a significantly higher number of transactions • Assign fees to new transactions or make it difficult for a node to process a large number of transactions

5.6 Sidechains

CHALLENGES	GOOD PRACTICES
Fraudulent transactions	• Require the use of merged mining, where the proof of work applied to validate the parent chain may also be used to submit valid blocks for the sidechain

5.7 Permissioned chain management

CHALLENGES	GOOD PRACTICES
Central authority key loss A node getting enough power to validate transactions of their choice – potentially fraud	• Monitor if one of the nodes increases processing power and is processing a significantly higher number of blocks • Use a clear set of criteria to accept new members, as well as to remove existing ones • Enable the use of recovery keys

5.8 Denial of Service

CHALLENGES	GOOD PRACTICES
Spam/invalid transactions being introduced for validation Slow processing of transactions	• Restrict which nodes can offer new transactions for validation • Assign fees to new transactions or make it difficult for a node to issue large numbers of transactions • Accept transactions from only authorized IP addresses • Have the possibility to block IP addresses as necessary

5.9 Wallet Management

CHALLENGES	GOOD PRACTICES
Key theft Unauthorized access to data	• Make sure the software for the wallet does not leave the key accessible in plain text outside the application • Require the implementation of recovery keys

Information disclosure Block/Compromise of operations of entity	

5.10 Scalability

CHALLENGES	GOOD PRACTICES
Slow processing of transactions Unexpected growth of the distributed ledger database	• Use sharding to allow specific transactions to be validated by specific entities • Use pruning to limit the growth of the ledger • Restricting the type of information allowed on the ledger and the entities allowed to act as full nodes

5.11 Governance Controls

CHALLENGES	GOOD PRACTICES
Institutions engaging in a not permitted activity	• Use smart contracts to allow for certain entities to engage in certain activities. • Internal governance procedure must enable internal identification of the individual signing off the request

5.12 Smart Contracts

CHALLENGES	GOOD PRACTICES
Unwanted behaviour of smart contracts Malicious software spread	• Use code review for smart contracts • Standardization of regular functions into libraries • Keep a library of approved smart contracts • Participants could use consensus protocol which considers a malicious program as an invalid state

5.13 Interoperability

CHALLENGES	GOOD PRACTICES
Fraudulent transactions	• Use pegged sidechains

6. Open Challenges

We have identified some issues that we believe could be improved or where the technology needs to evolve.

OPEN CHALLENGES	RECOMMENDATIONS
Information security standards • to keep data confidential • what and how data needs to be deleted from the ledger	• The Industry in cooperation with the regulators to define what to be kept confidential in order to remain compliant with regulatory requirements, such as General Data Protection Regulation, as well as sector or local regulations • The Industry in cooperation with the regulators to identify or develop standard methods for removing data from a ledger
Monitoring illegal activity	• The Industry to explore how current anti-fraud and anti-money laundering technologies need to be adapted or new ones created to work with the distributed ledger.
Interoperability between different distributed ledger protocols	• The Industry should explore the possibility to standardize requirements and harmonization of interoperability of different distributed ledger protocols • XML standards could potentially be good candidate for data operability
Quantum computing	• The Standardization bodies in cooperation with the Industry to research the use of post-quantum algorithms for asymmetric cryptography
Privacy preserving smart contracts	• The Industry to research availability of contracts preserving privacy, e.g. smart preserving contracts[21]
Governance controls	• Financial regulators in cooperation with the industry to explore mechanisms to add assurance and governance controls (standard legal and compliance items)
Wallet Management	• Industry to explore the possibility for creating standards for wallet software to store multiple keys from different distributed ledgers

[21] Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." University of Maryland and Cornell University (2015).

Annex A: Blockchain Use Cases

Blockchain technology holds a significant promise for the financial sector. It simplifies many types of business transaction and has significant applications within the non-financial sector.

A.1 Executing and settling contractual agreements

The current process behind an investment in shares requires for counterparties to hold both a bank account and their shares with institutions that can assist with the settlement of their trade. In contrast, a share trade accomplished through a distributed ledger can be settled instantly. Furthermore, as soon as a user receives their share tokens, is able to receive dividends and vote on proposals from the originating company. A share token is a digital version of a share certificate. However, rather than owning a paper certificate specifying ownership of shares, a shareholder owns digital tokens, representing the equivalent of shares. Due to the fact that smart contracts are legal contracts embedded in code, it therefore becomes possible to assign the attached rights to various classes of shares to these tokens.

In the case of more complex financial instruments such as derivatives, it is possible to program the execution of settlements following external events. Additionally, what were previously complex paper contracts can now be encoded into software, allowing financial institutions to assign a data-based framework to keep track of liabilities.

A.2 Reconciling and auditing information

Current processes require a financial institution to reconcile data internally then across business lines. Using Blockchain technology, institutions can eliminate double-entry accounting by connecting Back-office transaction processing to the initiator of a transaction. Furthermore, instead of preparing cyclical reports and audits for regulators, it will be possible to communicate data in real-time, allowing for a more efficient implementation of regulatory requirements and risk monitoring.

A.3 Signing messages on behalf of a counterparty

A good example of this is undertaking a proof of funds action. Whereas a client involved in import/export financing would need to request a letter from their bank, they can now sign a message on the Blockchain to prove they have the funds available. One way to do this is to simply transfer the funds to another wallet which the user has access to. In advance of the transaction, and then inform the counterparty of the wallet addresses to monitor. Other users on the Blockchain will only be able to identify that a transaction between two anonymous public keys has happened. Furthermore, it is technically feasible to encrypt the amount of a transaction, thus obscuring amounts to third parties.

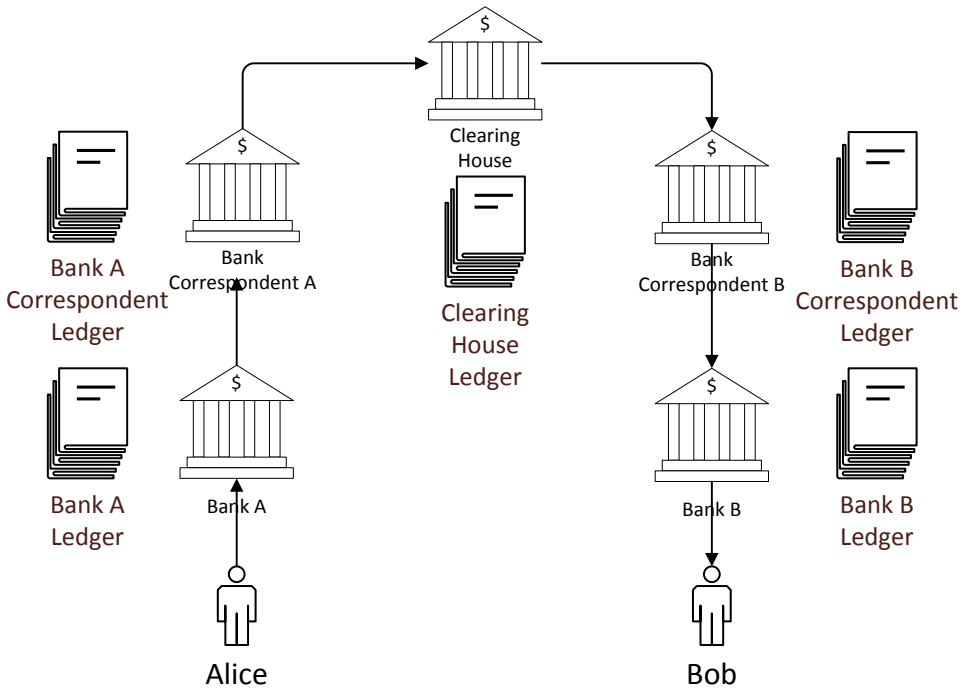
A.4 Connecting systems to IoT enabled devices

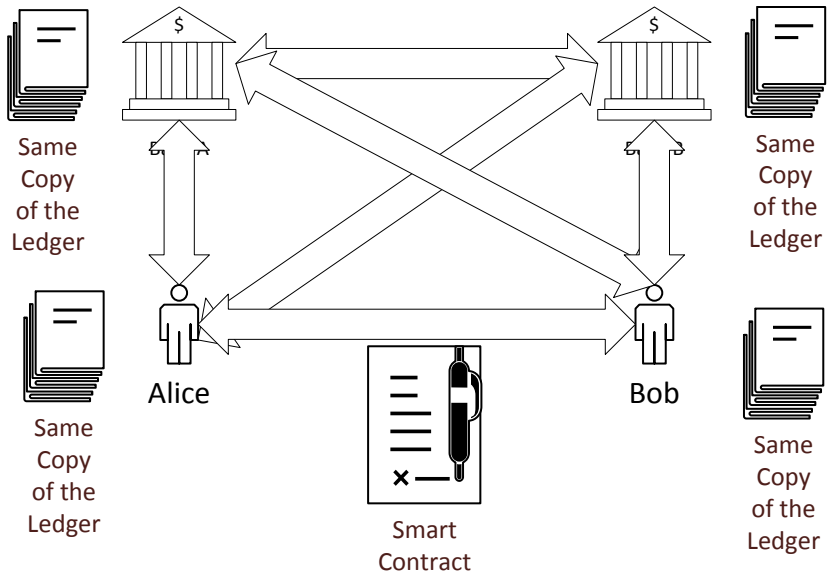
Blockchain technology will facilitate the development of large amounts of connected devices. By enabling their systems to interface with the data generated for these devices, financial institutions can obtain real-

time data for a range of matters such as destructive weather (for insurers), client location (fraud prevention), production facility status (valuation of a business).

A.5 Facilitating the transfer of assets

Registering and transferring the ownership of an asset can be a complex process involving multiple information silos. In the case of a residential property, relevant surveys must be carried out and intervention of a central counterparty, such as the Land Registry, is required in order to effectively record the transfer of ownership. A distributed ledger may enable property titles to be freely exchanged and linked to smart objects, such as an electronic lock that only opens for a specific key. Because the ledger is timestamped, it would also be possible for an arbitrator to verify who made the first claim in the case two counterparties were in dispute over a property. As soon as a property is transferred, this could also be made visible to the property buyer's bank, who would then be able to offer a variety of collateral-backed financial products.





A.6 Automating regulatory compliance

Prudential regulation defines the capital requirements needed by financial institution to function effectively. If all trades are happening on distributed ledgers with the information encrypted to transaction counterparties and the regulator, it becomes possible to calculate in near real-time an institutions' financial position and whether additional transactions will cause it to exceed the defined risk management parameters and capital requirements. Another application from a regulatory perspective lies in enforcing sanctions and closing access to specific markets if participants do not meet the criteria.

A.7 Portable Identity

Distributed ledgers have the advantage of using cryptography rather than user credentials. This means that participants in a ledger can produce their own identity by generating a private key only they have access to. The entity (individual or business) can then port its identity across different services as long as it uses the same address.

A.8 Automated companies and investment vehicles

Smart contracts make it much easier to conduct corporate governance. This includes automating the shareholder listing, recording board decisions and allocating assets. Financial institutions will be able to

take advantage of smart contracts by quickly instantiating investment vehicles on a distributed ledger whilst subjecting them to regulatory requirements. Because assets and funds can interact through a Blockchain, smart contract-based investment vehicles will be able to accurately manage the holdings of a business with full transparency.

Additionally, the issuance of new shares as well as trading of outstanding shares can be conducted through the ledger. Financial institutions can choose to trade within existing liquidity pools. However, their settlement can be linked to the Blockchain in order to improve the efficiency of trading activity.

Annex B: A study of the Ethereum DAO hack

Ether is the currency of the Ethereum Blockchain, with the second highest capitalisation in the digital currency market. Following its developer-focused Frontier release in July 2015, Ethereum released Homestead, the first production-grade version of the protocol, in March 2016. Since inception, Ethereum has been designed to allow for a range of applications rather than being limited to digital currency. A private version of the Ethereum network has even been used[22] by the R3 Consortium, a group of banks conducting an evaluation of Blockchain technology.

A range[23] of independently developed Decentralised Applications (DApps) are already in existence on the Ethereum network. These range from identity record lookup and validation to Blockchain-chartered companies, prediction markets and notary services. However, the main issue as with any new technology is that of adoption. Within the world of decentralised ledgers, this can happen in two ways, either bottom-up grassroots adoption or through the integration of Blockchain technology to the technology stacks of existing commercial service providers. The first major demonstration of the potential of a decentralised computer (Ethereum Virtual Machine) was the launch of the Decentralised Autonomous Organisation (DAO)[24]. This smart-contract based investment vehicle is aimed at providing a collective fund through which token holders can vote on investments and contractors to undertake specific ventures or tasks.

After a token sale (similar to IPO) in May 2016, the DAO raised over 11.5 Million Ether[25] (equivalent to over €140 million). This also represented over 13% of all Ether in existence at the time. On June 17th 2016, the DAO came under an attack known as a "recursive split."[26] Investors in a DAO can choose to separate from the existing vehicle and take their funds with them. In this case, a split function occurred, initiating a withdrawal. However, the function was called recursively, blocking the invocation of the function which updates the user's token balance, and therefore allowing them to withdraw more funds than they were otherwise entitled to.

In response, a protocol update[27] was proposed within the same month and adopted[28] on July 20th. This protocol reverted the previous transactions to an address accessible by the original DAO investors, enabling them to withdraw their funds. Within a day, nearly half the original investors had been able to recover their Ether.

The DAO hack is an example of how participants in a distributed ledger can, by consensus, overcome major security events. However, this also introduces the possibility of reverting past transactions, an issue which would mean that participants who transacted after the attack would have their transactions effectively nullified. This has resulted in a hard fork and the creation of a second Blockchain, "Ethereum Classic" which does not recognise the reversion of the attack as valid.

---

[22] Coindesk, *Ethereum Blockchain Project Launches First Production Release*, March 14th 2016
[23] Ethereum DApps
[24] DAOHub
[25] New York Times, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, June 17th 2016
[26] Hacking Distributed, *Analysis of the DAO exploit*, June 18th 2016
[27] Ethereum Blog, *CRITICAL UPDATE Re: DAO Vulnerability*, June 17th 2016
[28] Coindesk, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds,* July 20th 2016

Annex C: Distributed Ledgers

Bitcoin

The main cryptocurrency by market capitalisation and the most widely known implementation of the Blockchain concept, Bitcoin has operated without any central authority since 2009. There are now over 15m bitcoins in existence, with a market capitalisation of close to 8Bn Euros.

Bitcoin contains a very basic scripting language, called Script, making simple smart contracts a possibility. Script does not support loops and acts mainly as a tool to place parameters on how Bitcoins can be spent once they arrive at their destination.

Bitcoin uses a distributed ledger of transactions from which it is possible to compute the Unspent Transaction Output set, or UTxO. From a more practical perspective, this means that wallets' publicly exposed addresses (ie. unique identifiers) are not simply links to a set amount or asset. Rather, they are the most recent link in a publicly verifiable historical trail of transactions which ends at that address.

Open networks such as Bitcoin need to allow for an unbounded number of participants. The challenge that therefore arises is for a large number of parties who do not know each other and may not trust each other to arrive at an agreement about the truth of a given transaction. Bitcoin solves this problem with the use of a proof of work algorithm. In order for messages to be considered valid, they must be compressed into a block of data, which is appended to the existing database. This concept of validating a set of messages is referred to as mining.

The economic connotation of the term of mining refers to the fact that in the Bitcoin implementation, peers are given an incentive to maintain the system. Each new block in the Blockchain is the result of a competition by miners to provide a valid set of transactions in a block. Miners that successfully submit the next block receive a reward, denominated in the crypto-token linked to that specific Blockchain. For example, every 10 minutes on average, one of the miners on the Bitcoin Blockchain currently receives 12.5 Bitcoin (approx. 6 700 Euros[29]) for solving the current block.

For the system to function, peers must be able to ascertain that the information they have been presented with is truthful. Additionally, there should be a disincentive for dishonest actors to overtake the system. The proof of work function makes it unlikely for 2 parties to arrive at a valid conclusion to the challenge at the same time. However, it remains a possibility. When this happens, a fork may develop in the Blockchain with two separate chains proceeding. To stop these forks from continuing, and to ensure there is only ever one chain, clients accept the longest chain above all others. As a result, the two chains at the fork enter a race condition to see who can become the longest first, with the smaller one being discarded.

The issue that arises with a distributed ledger is guaranteeing that, as the dataset evolves over time, older data is not subject to modification. To avoid this, all previous blocks in the system are included in the hash for the most recent block. This is referred to as a Merkle proof[30][31]. The Bitcoin implementation features a chain of blocks. Each block contains a block header with 6 elements:

[29] Based on an XBT/EUR rate of € 533.92 on Aug. 8th 2016
[30] US Patent No 4309569, Filed September 1979
[31] Ethereum Blog, *Merkling in Ethereum*, November 15th 2015

- Block version - Specifies the version of the Blockchain the mining software is generating for.
- Hash of previous block header - A hashed version of the previous block header.
- Hash of Merkle Root (Transactions in Block) - A hash of all transactions/messages in the current block.
- Timestamp - The time of publication of the block.
- Bits - A 256 bit number that acts as a target for miners to produce a hash under the value of in order to generate a valid block.
- Nonce - A random number to allow for different hash outputs for a block on each attempt.

In order to produce a block, miners pick a set of transactions to validate and hash them using a SHA-256 algorithm. If the resulting hash is a lower number than the Bits, then it is considered a valid solution and is broadcast to the rest of the network. If it isn't, the nonce is changed for each hashing run until an output lower than the Bits is found.

The algorithm used for proof of work requires the entity running the computation to contribute computational power. The probability of submitting the valid solution to a block is proportional to the total amount of computing power contributed by that user during the time window necessary to find the most recent valid block. The proof of work algorithm has enabled Bitcoin to operate for over 7 years. However, one of its main flaws resides in the fact that it consumes a large amount of energy. The first unintended consequence is that this creates a drive towards centralisation of mining capacity due to economies of scale to be achieved on hardware and electricity. Additionally, based on current projections, Bitcoin may consume as much electricity as Denmark by 2020[32]. As such, research for other needed solutions has resulted in alternative proposals that can lower electricity consumption without impacting data security.

Ethereum

Ethereum was founded in 2013 and launched in 2015 after a successful crowdfunding campaign which raised over $18m in Bitcoin. To date there are over 80m Ether in circulation, with a market capitalisation approaching 1Bn Euros.

Ethereum offers the same range of computational abilities as existing real-world systems, and in particular supporting loops and conditional statements. The inherent design of the system means that smart contract code and its' execution are open for review by all parties. Ether is a form of payment made by the clients of the platform to the machines executing the requested operations.

A variety of languages have been developed to support smart contracts. Ethereum's virtual machine runs on byte code, which can now be compiled out of many traditional languages including Javascript and C++. Solidity is a new High Level Language developed specifically for Ethereum contracts, similar to Javascript, designed to make complex smart contracts as easy to write as possible.

Whereas Bitcoin blocks contain transaction messages, Ethereum blocks contain messages representing computational steps of the execution of a smart contract. This computation is funded by subunits of Ether, more commonly referred to as "gas". All execution fees are paid by the entity issuing the instruction and are included within the mining rewards for that specific block. Blocks on the Ethereum chain are currently also validated using a proof of work algorithm; however, it is in the process of switching to Proof of Stake.

[32] Breitbart, *Bitcoin may consume as much electricity as Denmark by 2020*, April 3rd 2016

Ripple

Already in use by a number of financial institutions, Ripple[33] provides a Peer to Peer system for banks in foreign exchange (FX) markets to transact with each other. The global ledger is replicated by thousands of participants. FX trades take place through a distributed order book, where all bids and asks are recorded and executed. Ripple relies on the concept of "gateways". Hence, in order for a user to move their fiat (i.e. account balances denominated in government-issued currencies such as EUR, GBP etc) balance out of the Ripple network, they will need to request a settlement from the entity that initially issued that balance on the network. Therefore, Ripple still contains a degree of counterparty risk as users are required to trust that they will be able to receive an effective settlement of their funds.

Hyperledger

The wide variety of applications for distributed ledger technology also means there is a large amount of potential optimization to be done, as some protocols may be more appropriate in certain circumstances depending on who is building them and for what. Recognition of this has led to the development of Hyperledger, which is being developed by a consortium of finance and technology companies, led by the Linux Foundation. **Hyperledger[34] is focused on developing a standard for distributed ledgers that will allow separate ledgers to communicate with one another without needing bespoke APIs**. From a security perspective, Hyperledger uses two types of certificate:

- Enrolment certificates: Controls a participants' access to the network
- Single use Transaction Certificates: Restricts the ability to push undesirable transactions

Hyperledger refers to this common standard as Fabric, and intends for smart contracts to be writeable on this platform in any common programming language. The aim is to produce a completely modular system that will allow everything – from the cryptography used to the underlying consensus protocol – to be easily customized and deployed with as little effort as possible. The key driver of Hyperledger's modular approach is to allow business participants to determine the consensus protocol to use, following their business needs.

Sawtooth Lake/Intelledger

Sawtooth Lake[35] is an open source project developed by Intel, who are also participating in the Hyperledger initiative. Founded on the same principles as Hyperledger, but with a slightly different focus, its' primary goal is to operate on IoT devices with limited human involvement.

Sawtooth Lake abstracts the core concept of consensus by isolating consensus from transaction semantics. It provides two consensus protocols with different performance trade-offs; Proof of Elapsed Time and Quorum voting, an adaptation of the Ripple protocol.

This project is currently in early development, with an alpha release simulating the token generation function of the segregated secure CPU unit without the actual underlying hardware. However, some key questions remain about this system, including Intel's access and knowledge of the cryptographic keys on the hardware. Additionally, it is not clear whether or not it is possible for a hacker to extract the keys to

[33] Ripple, *Executive Summary for financial institutions*
[34] Hyperledger Foundation
[35] Intelledger developer documentation

create timestamps that will assure them victory in the consensus determining lottery by decapping the chips. Another question that remains is whether or not the range of hardware that will work in this system can be expanded without being vendor-locked.

Corda

Corda is a distributed ledger for contracts tailored for use by financial institutions. It rethinks a number of the assumed required components of their design. Transactions/agreements, are only visible to parties with a need to see them, including a definable regulator. In this setting, the regulator could be an authority such as the European Banking Authority or an industry body defining a set of standards market participants are required to adhere to. Corda[36] has no cryptocurrency, as these parties alone are also the validators of the agreement taking place, with multiple consensus mechanisms potentially being used.

Corda aims to provide a global distributed ledger, where transactions serve as authoritative and binding facts to ascribe contractual obligations to counterparties[37]. To this effect the behaviour of the system is designed in code and backed by a legal framework which outlines the obligations of participants. Corda is designed to allow a number of financial transactions, including enabling financial institutions to issue digital fiat currency to counterparties. In turn, these Blockchain-based funds can be used for trading and settlement.

[36] R3 Blog, *Introducing R3 Corda a distributed ledger designed for financial services*, April 5th 2016
[37] R. G. Brown, J. Carlyle, I. Grigg, M. Hearn, *Corda: An Introduction*, August 2016

Glossary

Decentralised Autonomous Organisation (DAO)
A DAO is an autonomous entity with programmable rights deployed on a Blockchain as a smart contract. A DAO serves as a proxy to represent a real-world entity or grouping of entities.

Proof of Elapsed Time
As part of its Intelledger proposal, Intel has devised a means of establishing a validation lottery that takes advantage of the capability of its CPUs to produce a timestamp cryptographically signed by the hardware. Whoever in the ecosystem has the next soonest timestamp will be the one to decide which transactions will be a part of the next block in the chain. This consensus method is extremely energy efficient compared to Proof of Work and therefore more adapted to IoT devices. Proof of Elapsed time does not require a Public Key Infrastructure. Assets with compatible hardware can simply be added to the network and immediately participate in the validation process.

Ripple Protocol
The Ripple consensus protocol operates a ledger system. The last closed ledger is the most recent ledger validated by the consensus process and can be accepted as representing the current state of the database. In order to validate new transactions, servers amalgamate outstanding transactions into a "candidate list." All participants then vote on valid transactions to be included in the ledger. Transactions that meet the 80% threshold of "yes" votes are included within the following last closed ledger state.

Proof of Work
Proof of Work uses computational power to validate new blocks of data. To participate in this scheme, participants are required to collate transactions within a single block and then apply a hash function with the use of some additional metadata. If the resulting hash falls within the acceptable range set by the current difficulty parameters of the proof of work scheme, then that block is considered valid and is broadcast to the rest of the network as a valid submission. The probability of creating a valid block for any individual miner is defined by the proportion of computing power held by that miner in comparison with the rest of the network.

Proof of Stake
This consensus protocol is based on the validators voting on valid blocks whilst posting collateral in order to be able to participate in the validation process. Unlike Proof of Work, Proof of Stake relies on proving the user is invested in the underlying token of value of the network being mined rather than being the owner of a large amount of computing power. Ethereum will use the Casper protocol variant. This implementation of Proof of Stake sees all validators on the network undergo an iterative voting process on the next valid block. Votes are made in the form of cryptocurrency, which is locked as a deposit until consensus has been reached. The next valid block is the one which has the majority of deposits (at least 51%) allocated to it. Due to the iterative voting process, a validator that suddenly switches their vote to a completely different block may forfeit their deposit. Proof of Stake additionally allows miners to focus computing resources on processing more transactions per second rather than producing a large number of hashes as in Proof of Work.

Quantum Computing
Quantum Computing is a new computing paradigm. It involves the use of quantum based phenomena. One of the main benefits is opening the way for even smaller computers. This is especially relevant due to

quantum tunnelling, an issue which arises for chips below 10nm as electrons begin to jump across closed transistor gates. Quantum computers use “qubits” instead of conventional bits of information. These qubits may take the form of an electron trapped inside a cage of atoms or the polarisation of laser light. Other forms of quantum computers involve using molecules and observing their spin in order to reconstruct information. Although quantum computers may potentially offer exponential computing capabilities for specific tasks (such as brute-forcing attacks), they are still highly experimental.

Reconciliation

Reconciliation is the process by which individuals, companies and institutions must ensure all records are valid and all instructions effectively executed. Reconciliation firstly involves ensuring all the internal data of an organisation has been correctly captured and is in line with existing policies and rules. The second element involves ensuring that, where data is shared with external counterparties, both parties hold the same copy of that information. Blockchain technology promises for a large simplification of the reconciliation process as data will be shared at the point of origin.

Double Spend

Double-spending is the result of successfully spending some money or an asset more than once. Double spend attacks can mainly occur when the network has not yet processed a previous transaction from an address.

Unspent Transaction Output Set (UTxO)

One of the key elements of a Blockchain is that data is considered valid in reference to previous data. Hence, in the example of Bitcoin, the UTxO is the list of all current Bitcoin addresses which have previously received funds and have not yet been spent. Each address can be linked to all the previous transactions that resulted in the funds being routed to that address.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-05-16-076-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-200-4
DOI: 10.2824/80997