WTO
Global Trade and Blockchain Forum

What is Blockchain and DLT?

Virginia Cram-Martos

Geneva, 02 December 2019

What is Blockchain and DLT?
Our Agenda

1. What is a Blockchain and Why Should Governments Care?
2. An Introduction to Blockchain Terminology
3. Critical Factors

1. What is Blockchain and Why Should Governments Care?

= Just One Blockchain Out of Many

Blockchain

= A Distributed Ledger Technology (DLT)

= The principal, most tested DLT

An example of another DLT is the IOTA Tangle

Not all Blockchains and DLTs are equal, they vary in:

- **Vulnerability** (to hacking and other system failures)
- **Robustness** (how well they handle problems such as flawed code or being hacked)
- **Cost** (transaction cost, sometimes referred to as «gas»)
- **Speed and ability to scale up** (to large transaction volumes)
- **Degree of Privacy** (pseudo anonymity vs total anonymity)

What are the Benefits?

Blockchain has the potential to significantly improve asset and information management through

- **Immutable and verifiable transactions and time "stamps"** allowing the elimination of paper where today it is still required;
- **Automated (and immediate) reconciliation** algorithms facilitating faster payments and improving accountability
- **The tracing of digital assets through 100s or 1000s of transactions** supporting the tracking of goods, for example because they are sensitive/regulated or to ensure the sustainability of their origin (for example, to prove that wood comes from a sustainably managed forest)
- **Immutable "original" information which can be used for identities, reputations, electronic certificates, licenses, etc.** facilitating access to benefits, reducing fraud and speeding up regulatory procedures.

Blockchain Technology will profoundly change trade and government business models

Through

1. The creation of “original” electronic documents and assets
2. High traceability
3. Instant reconciliation
4. Increased transparency

Creation of "Original" Electronic Documents and Assets

Blockchain can be used to create

- **Electronically "notarized" original electronic documents or agreements such as contracts, certificates, diplomas and licenses**
- **Including a time stamp and a "guarantee" that no changes have been made since the time of issuance**
- **These "originals" may include assets, such as titles to property, like bills of lading which can also be bought and sold over a blockchain**

High Traceability

TriAngulArity

To illustrate this capacity, take the Bitcoin (or any cryptocurrency) application

For each individual crypto-coin, its blockchain automatically tracks every transaction, including the date, and time and the participants – that is how the blockchain knows who owns a crypto-coin at any moment in time.

In Bitcoin, transaction participants are pseudonymous (act using a pseudonym that provides anonymity as long as the owner of the pseudonym is not revealed). But a Blockchain network can also be designed so that every participant is known.

Now, take the crypto-coin and replace it

with the "digital twin" (digital representation) of a product, such as a diamond or a shipment or a container full of shipments or a publicly procured good, such as an office computer

<u>Imagine</u> the possibility for tracing every transaction involving that document or good and, if relevant, knowing the identity of the participants

“Instant” Reconciliation

TriAngulArity

The traceability function of blockchains results in the network knowing the exact balance of crypto-coins owned by every node/participant.

In other words, this property can be used to automatically create audit trails, at a low cost even for complex, multi-party, multi-location transactions which are spread out over time.

Now, <u>Imagine</u> this capacity being used to track and calculate charges/balances for

- **Shipping containers**
- **The origins of different product components**
- **Goods with certified characteristics (fair trade, organic, sustainably farmed, etc)**
- **Costs along a supply chain**
- **Implementation of large and complex contracts with multiple shipments, receiving documents, payments, etc.**
- **Insurance revenues and payments**
- **Budget expenditures (by projects, departments, agencies, etc)**

Increased Transparency

The immutable aspect of blockchains means that

1) If the rules are changed/updated
2) If the data changed/updated

<u>Everyone who can access the blockchain will know what was changed, by whom and when</u>

These are characteristics which also make blockchains highly auditable and may change the nature of auditing from being one of checking data “after the fact” to checking to be sure that the system’s rules are correct.

2. An Introduction to Blockchain Terminology

Commonly Used Terminology*

Triangularity

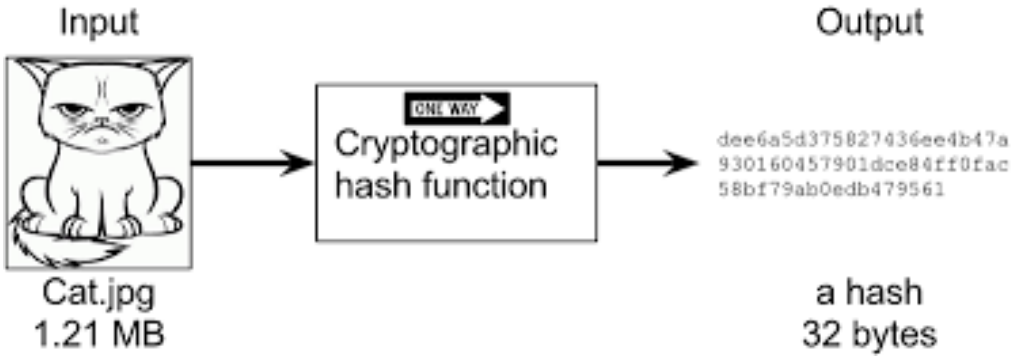
- Satoshi Nakamoto
- Hash
- Block
- Node
- Validation
- Consensus, Forks and Consensus Methods
- Permissioned (Private) & Permissionless (Public) Chains
- Public and Private Keys
- Cryptocurrency,
- Tokens and Digital Twins
- Fiat Currency, Stablecoins & CBDCs
- On-Chain and Off-Chain
- Smart Contracts and Oracles

* http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf

Satoshi Nakamoto – Inventor of Bitcoin

- In October 2008 an author, or a group of authors, under the pseudonym *Satoshi Nakamoto* published *a* White Paper called, “Bitcoin: A Peer-to-Peer Electronic Cash System”
- On 9 January 2009, Satoshi Nakamoto released Version 0.1 of the Bitcoin software, which is **open-source** and was the first software to implement the principles described in the October 2008 paper.
- Satoshi Nakamoto continued to collaborate on the Bitcoin software until mid-2010 when he handed over control of the source code repository, updates and several related Internet domains to other prominent members of the bitcoin community and, in 2011, stopped his involvement.
- Up until today, no one has discovered his true identity.

Hashes



A Hash is the result of mathematical operations carried out on the numeric representation of data—all data in a computer being numbers. The result is a unique cryptographic fingerprint of the data.

Given the data and the algorithm used – one can quickly confirm that no changes, at all, have been made because if the result is the same, the data is the same.

A hash is a one-way function, which means it is almost impossible to recreate the original data if all one has is the hash (i.e. reverse engineer it).

ISO and other organisations publish standard hashing algorithms

Blocks, Nodes and Validation

- **Block**: Data that is appended to the ledger after validation. Once a block is written to the chain, it cannot be changed or deleted without replacing all subsequent blocks.

- **Node**: A system that hosts a full copy of the blockchain ledger. In some blockchains, such as Bitcoin and Ethereum, all nodes participate in the consensus process, in others it may be only be selected nodes.

- **Validation**: This is the process of verifying that the data in the new block is correct – for example that someone is not spending more cryptocurrency than they have and that the previous data in the blockchain has not been changed.

Consensus and Forks

- **Consensus**: this is the method used in blockchains for validation. It means that all participating nodes must agree on a block before it is added. After 51% of the nodes agree, any node that does not agree no longer belongs to the blockchain. The more nodes a blockchain has the harder it becomes to cheat by controlling 51% of the nodes and, so, the safer it is considered to be.
- **Forks:** If one or more nodes “insist” on disagreeing, then their version of the blockchain “forks” from the original and becomes a new blockchain – it is like a fork in a river, the 2 blockchains share the same data stream up until the block where they fork. Nodes on the forked blockchain cannot directly transact with those on the original blockchain and vice versa
- In some blockchains all nodes participate in the consensus process (e.g. Bitcoin and Ethereum), in others it may be only be selected nodes.

Consensus Methods (1 of 2)

- There is a lot of research looking at how to find the most efficient, secure (from hacking) and scalable consensus method. Some believe that these form a triangle and only two sides can be maximised, i.e. if a consensus method is highly secure and efficient then it will not be scalable (i.e. it will be slow), or if it is scalable and efficient, then it will be less secure.
- The most common, well-known and tested method is the one used in Bitcoin. It is called "**proof of work**" (PoW) whereby nodes compete to add blocks to the chain by solving a difficult computational problem. It requires a great deal of computing power, or great luck, to be the first to solve the problem. If you are first, other nodes check your work and if more than 51% agree, your block is added.
- This process is called **"mining"** because a node is rewarded with cryptocurrency if it succeeds in adding a block.

Consensus Methods (2 of 2)

- Another popular form of consensus is **“proof of stake”** (PoS). In PoS a miner is limited to mining a percentage of transactions that reflects his or her ownership stake. For example, a miner who owns 2% of the Bitcoin available can mine only 2% of the blocks.
- With PoS, an attacker would need to obtain 51% of a blockchain’s cryptocurrency to carry out a 51% attack. PoS makes it disadvantageous for a miner with a 51% stake to attack the network. First, it would be difficult and expensive to accumulate 51%, and second, a miner with 51% stake in a coin would not want attack its network because then his majority share would fall in value
- These are only the two most commonly used and mentioned Consensus methods/protocols. There are many others, especially in private/permissioned networks where participants worry less about 51% attacks.

Permissionless (Public) Chains/Ledgers

- **Permissionless(Public) Blockchains,** Anyone can participate in the consensus method, implement a transaction (write to) or read the information on a public blockchain without needing permission. Bitcoin, Ether and a range of other cryptocurrencies with capitalizations going up to 59 billion USD operate this way.
- Public blockchain ledgers are designed to operate according to rules that do not require governance or regulatory mechanisms, because those mechanisms might themselves be exploited for antisocial outcomes—for example, if a governance mechanism were to be hacked by a third party or abused by a trusted regulator. Public blockchains operate with absolute trust in their algorithms and are designed to avoid any need to trust counterparties. This is why they are sometimes referred to as being **trustless**.

Permissioned (Private) Chains/Ledgers

- **Permissioned (Private) Blockchains** come in 2 flavours:
  1) Permission is needed to write but anyone can read
  2) Permission is needed both to write and to read

  In both cases, where permission is required, a participant's profile with what they are permitted to do is registered on the blockchain and is controlled via a smart contract
- Private blockchain ledgers are the most common kind being implemented by business and governments for non-cryptocurrency applications
- Because private blockchains have more control over who participates they often use less secure consensus mechanisms that allow them to increase efficiency and scalability. Only time and experience will tell if this is a wise choice.

Public and Private Keys : Means of Access

Public/private key cryptography is used for identifying parties to a transaction and controlling access to data.

An analogy is email, where

- The **public key** is your email address which others can use to send messages to you
- The **private key** is your password which gives access to the private material, which is your messages

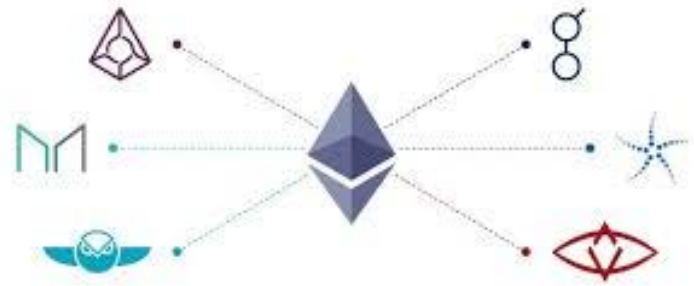
So, on a blockchain, a public key can be used, for example, to send a document or a payment to a party, but only the party with the private key can access those documents or payments after they are sent.

Cryptocurrency

CryptoCurrency is “a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank” (Oxford Dictionary.

A cryptocurrency **coin** exists on and is used to operate its own blockchain network, for example, Bitcoins, Ethers, Moneros. They can be used as payment, as a store of value, or for accounting. The website Coinmarketcap lists over 900 different coins.

Tokens and Digital Twins



TriAngulArity

Tokens are created on top of existing blockchains and are used to interact with decentralized applications (**dApps**). Fees need to be paid for all token transactions, using the coin of the underlying blockchain.

The most used, but not the only, token platform is Ethereum. Tokens built on Ethereum are known as ERC-20 tokens.

Tokens are often used to activate features of the application they were designed for. For example, Musicoin is a token that allows users to access features of the Musicoin dApp, like watching a music video. Other digital assets which tokens could represent are discounts, loyalty coupons, digital art, etc.

Some tokens are used to represent physical things. If you wanted to sell your house or car using a smart contract could you physically put them into the smart contract? No. So, instead, you can use a token to represent your house or car. **This is called a digital twin**

For a more detailed explanation of different types of tokens: https://www.bitdegree.org/tutorials/token-vs-coin/

Fiat Currency, Stablecoins & CBDCs

- **Fiat Currency** is a “traditional” currency backed by a central bank such as dollars, euros, yen, etc.

- **Stablecoins** are cryptocurrencies backed by a single currency or a basket of real currencies - deposited in a “real” bank. The objective of a stablecoin is to have the blockchain benefits, for example easily and cheaply traded assets and the use smart contracts, while avoiding the price volatility of cryptocurrencies.

- **CBDCs** are Central Bank Digital Currencies (so digital dollars, euros, yen, yuan, etc). Currently there are none, although some may consider the “petro” issued by Venozuela to be close. At the same time, there is a lot of discussion and “signalling” which indicates that this will eventually happen.

On-Chain and Off-Chain

- **On-Chain data and transactions** are data and transactions that are recorded directly onto a blockchain (and all of the distributed copies of that blockchain). If there is a lot of data, this can be expensive and can also “bloat” the size of a blockchain and make it less efficient.
- **Off-Chain data** is stored off of the blockchain but is related to what is written on the blockchain. For example, sometimes “pointers” to off-chain data are written on a blockchain or a hash and a time stamp is stored on the blockchain as a way of “notarizing” the off-chain information.
- **Off-Chain transactions** are similar to off-chain data. The results of a transaction may be recorded or “notarized” on a blockchain, or a blockchain smart contract may send an instruction to an off-chain application that triggers a transaction (for example the transfer of goods or a payment)

Smart Contracts & Oracles

TriAngulArity

Most non-currency Blockchain applications use Smart Contracts

Smart Contracts are computer programmes stored on a blockchain (so they cannot be changed) which automatically execute based on defined «events». These events are notified to the blockchain by trusted off-chain **«oracles»** which could be government agencies, or sensors or other reliable data sources

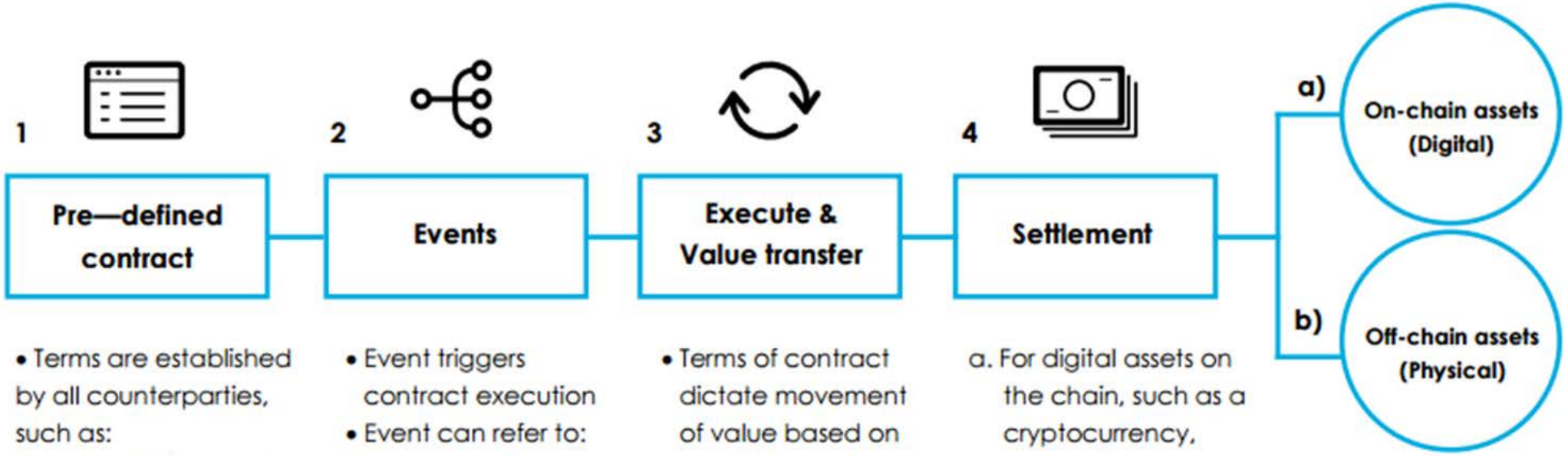
For example, if a sensor inside a container indicates that its temperature has exceeded a permitted level, a smart contract could send a request for an inspection or trigger an insurance payment.

Note: if you are designing an application, select your oracles carefully because they can be a serious «weak point»

Smart Contracts were invented in the 1990s by Nick Szabo; the proposal to programme a blockchain for implementing them was made by Vitalik Buterin in late 2013 who co-founded Ethereum which went live in July 2015.

ethereum

Smart Contracts are programmes on a blockchain that automatically execute based on defined «events»



- Terms are established by all counterparties, such as:
  - ◊ Variable interest rate (e.g LIBOR)
  - ◊ Currency of payments
  - ◊ Currency rate
- Conditions for execution (e.g time and date, LIBOR rate at given value)

- Event triggers contract execution
- Event can refer to:
  - ◊ Transaction initiated
  - ◊ Information received

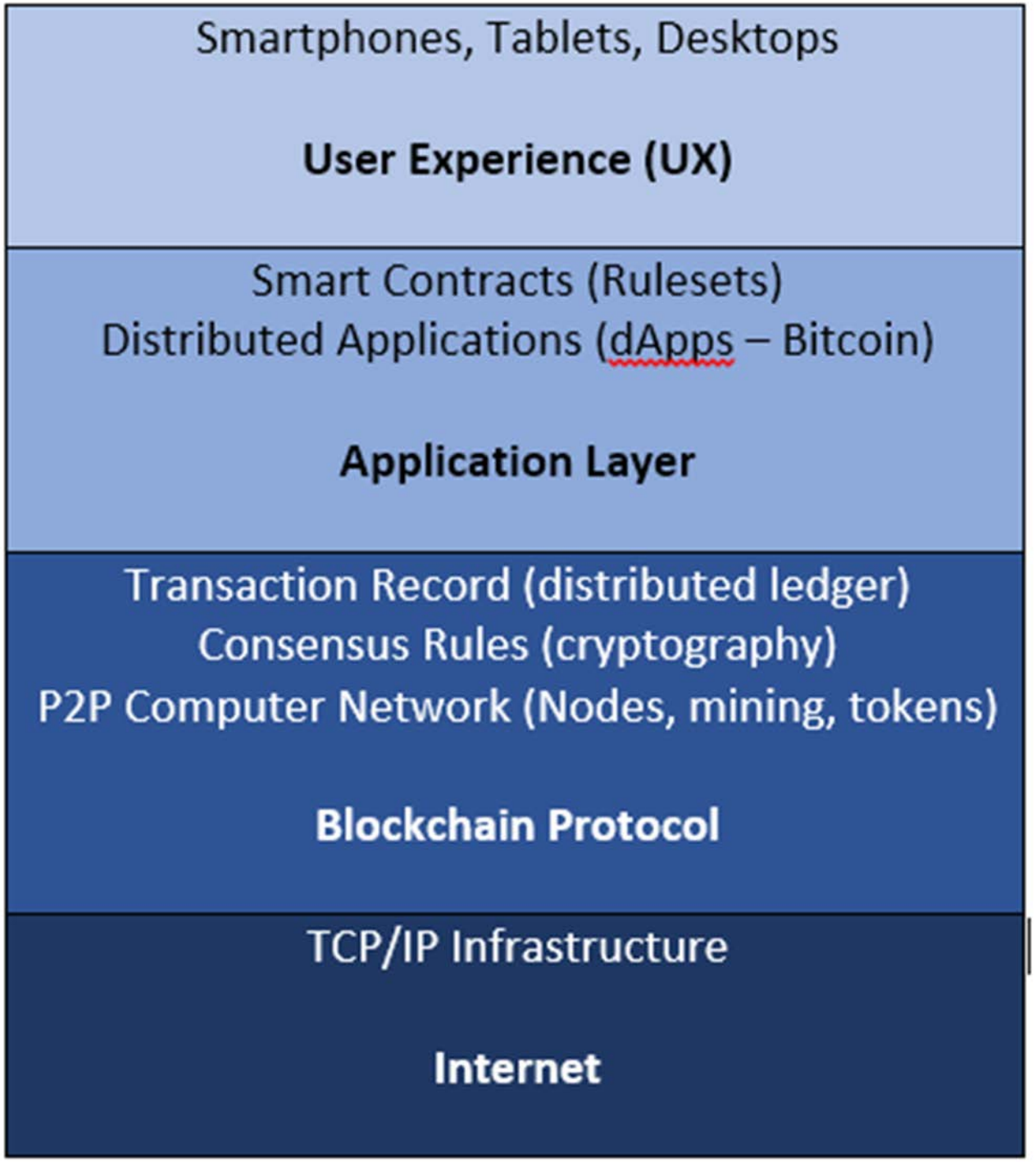
- Terms of contract dictate movement of value based on conditions met.

a. For digital assets on the chain, such as a cryptocurrency, accounts are atomically settled

b. For assets represented off the chain, such as stocks and fiat, changes to accounts on the ledger will match off-chain settlement instructions

Source: sharetheledger.com

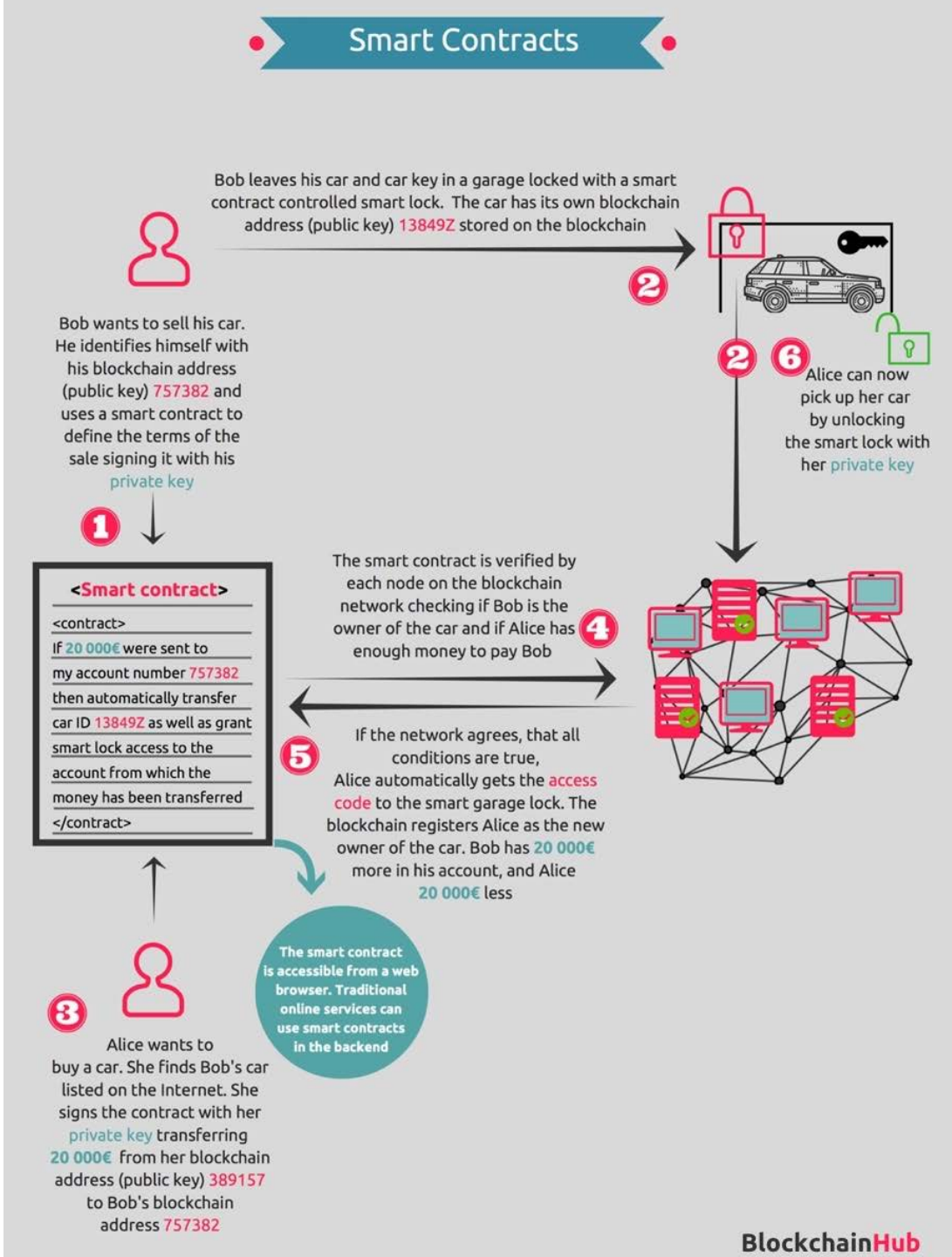
How do smart contracts fit into the overall blockchain context?



TriAngulArity

Most security flaws in blockchain systems occur in these top two layers and, especially, in UX

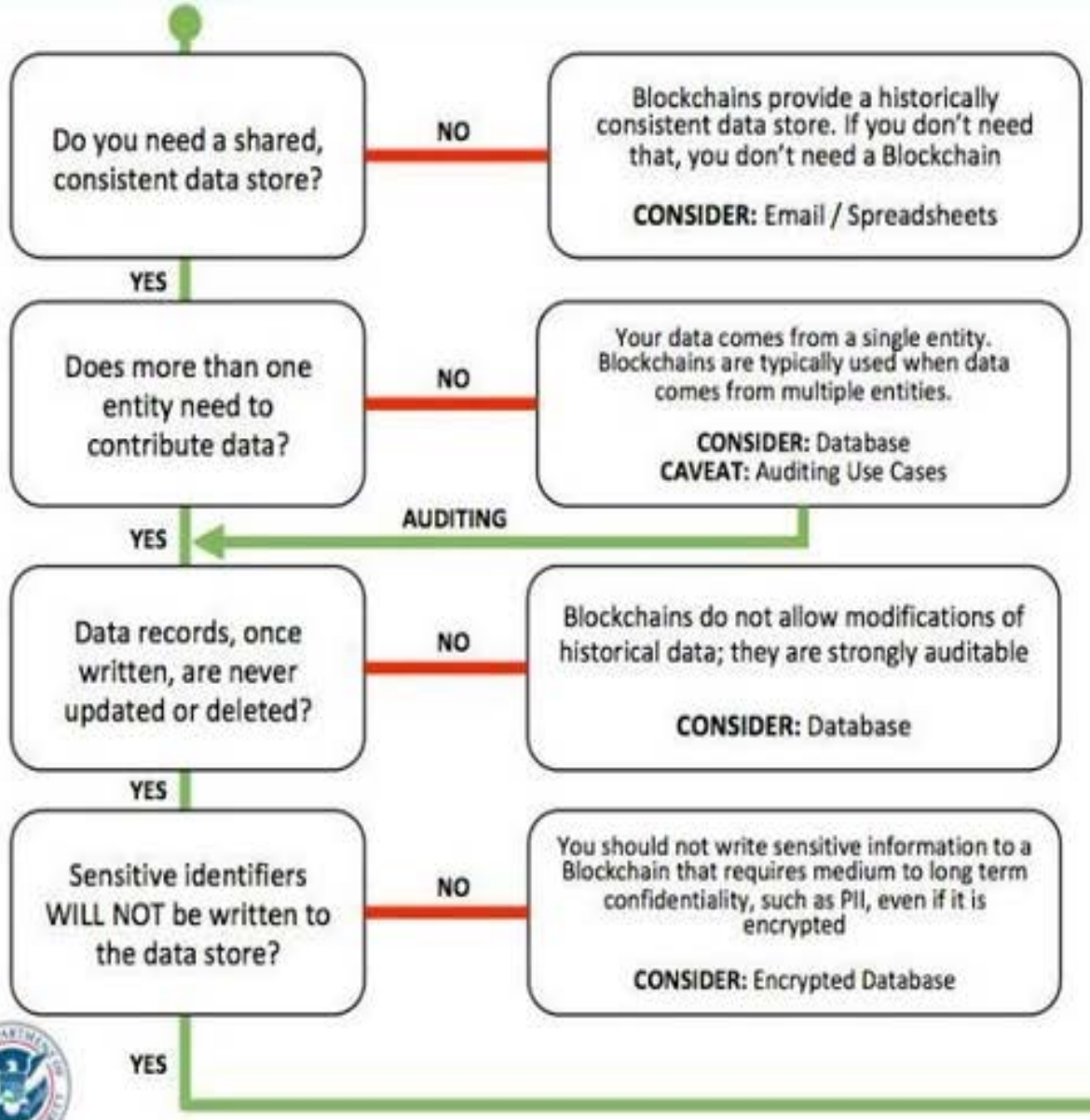
A smart contract example: purchasing a car

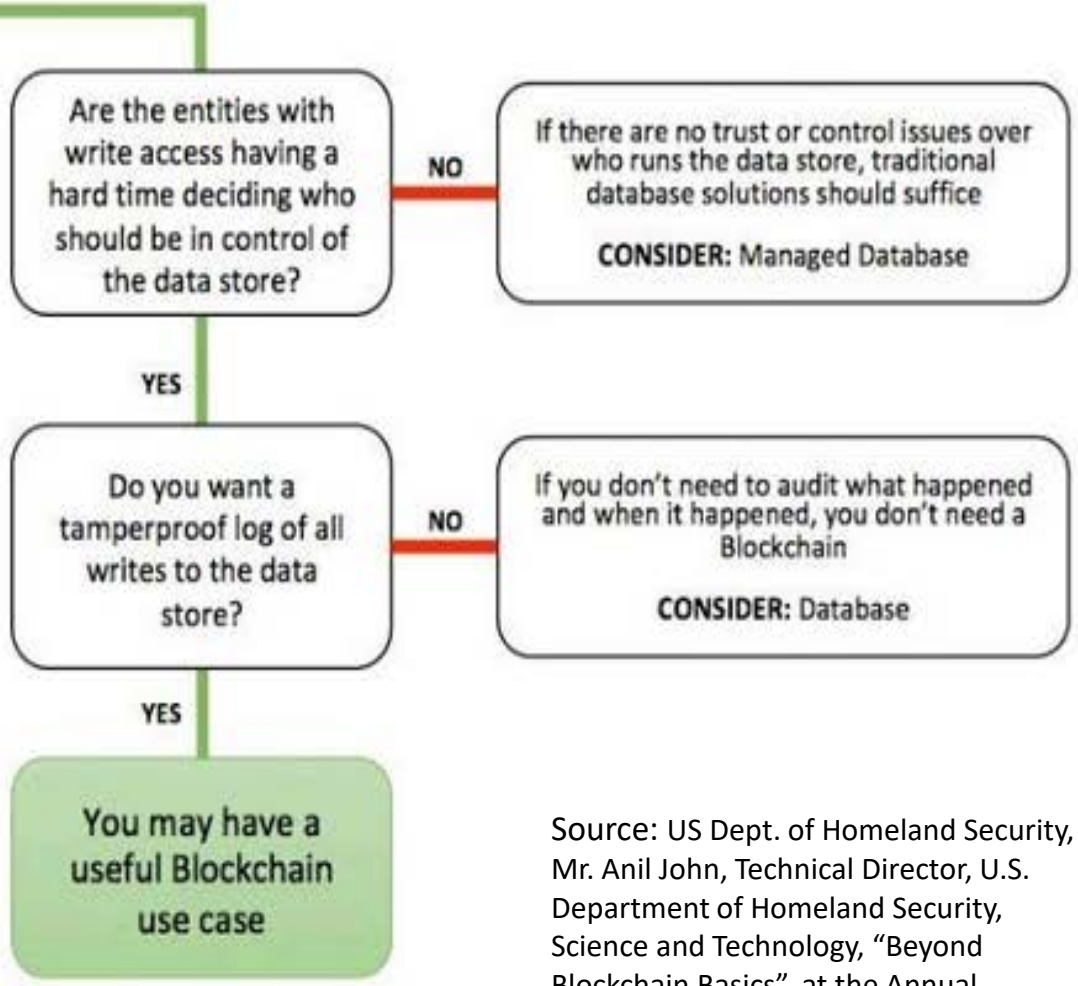


3. Critical Factors

Is Blockchain the «Right» Solution?

If only one of the answers on the right is «no», you may still have a case. For example, if a tamper-proof log is key or those with read access do not trust those with write access





Source: US Dept. of Homeland Security, Mr. Anil John, Technical Director, U.S. Department of Homeland Security, Science and Technology, "Beyond Blockchain Basics", at the Annual Computer Security Applications Conference, 5 December 2018

METI
Ministry of Economy, Trade and Industry

TriAngulArity

The original presentation by METI and the full report it is based upon can be found at:
http://www.meti.go.jp/english/press/2017/0329_004.html
Text that is in italics and underlined was added or changed

Evaluation Forms for Blockchain-Based System ver. 1.0

12 April 2017

Information Economy Division
Commerce and Information Policy Bureau

There are many Blockchains and many variations in blockchain technology

Typical classification of blockchain platform by governance scheme (this information changes regularly based on new research and technical developments)

*Modified from IBM release document

	Public	Consortiums	Large Corporates
Governance	*System Protocol*	Several parties	One single party
Identity of users	Open - Free	Permissioned (for write access or both write and read access)	
	Not specified, may contain malicious members	*Specified, composed of "reliable" members (who, nonetheless, if «hacked» could become malicious)*	
Consensus algorithm	Proof of Work, of Stake, etc.	Proof of Stake, PBFT (Practical Byzantine Fault Tolerant) or other	
	Slower-block confirmation Large electricity consumption	Fast block confirmation, Small electricity consumption	
Processing time of transaction	*Currently* Long (e.g. 10 min)	Short (e.g. a few seconds)	
Use case	Virtual currency, *Notarized documents, tokenized assets etc.*	Business network as interbank transfer, stock exchange etc.	
Example	Bitcoin, Ethereum etc.	Ripple, Hyperledger Fabric, etc.	

Items on Evaluation Forms for Blockchain-Based Systems ver. 1.0 (METI)

Large Category	Category	Evaluation items
Quality	Performance Efficiency	Throughput
		Network latency
		Block confirmation
		Data reference
	Interoperability	Interoperability with existing systems
		Interoperability with other blockchain systems
	Scalability	Throughput
		Network latency
		Capacity
	Scalability	Number of nodes
	Reliability	Maturity
		Availability
	Reliability	Fault Tolerance
		Recoverability
	Security	Confidentiality
		Integrity
		Non-repudiation
	Security	Authenticity, *Able to be authenticated*
	Portability	Adaptability
		Replaceability
Maintenance / Operation	Maintainability & operability	Modularity
		Reusability
		Analyzability
		Modifiability
		Testability
Cost	R&D	R&D of Blockchain platform technical elements
		R&D of subsystems
	Implementation (Commercialization)	Hardware cost
		Software cost
		System implementation cost
	Maintenance & operation	Operational cost
		Maintenance cost

These Items Are Closely Related To The Characteristics Of Blockchain Technology

The Evaluation of Blockchain Systems Depends Upon a Complex Set of Trade-offs Between Unique Characteristics

Descriptions of Many Key System Characteristics Can Often be Found in System «White Papers»

Some Additional Resources on “What is Blockchain?”

- https://www.coindesk.com/
  Introductory information is under «Blockchain 101»
- https://blockgeeks.com/
  Note: Don’t be scared by the very «techy» home page. Under search enter your question, for example «What is a smart contract?»

Use Cases Related to Trade

- Identity (legal entities, persons and things such as diamonds)
- Tracing of Goods and Shipments (Including Goods in Transit)
- Official documents (Bills of Lading, Certificates of Origin, Phytosanitary Certificates, etc.) issuance and related reconciliations
- Property registration (Containers, Trucks, Ships)
- Parametric Insurance for Damage to Goods
- Trade financing (letters of credit and invoice-based financing)
- Government asset monitoring and management (Customs Warehouses, Temporarily Impounded or Permanently Seized Goods, etc.)

Trustworthy Information Collection

The information needed for delivering government services often comes from a range of sources including:

- Multiple government agencies
- Different levels of government (federal, provincial, municipal)
- Semi-public or private organizations
- Citizens themselves

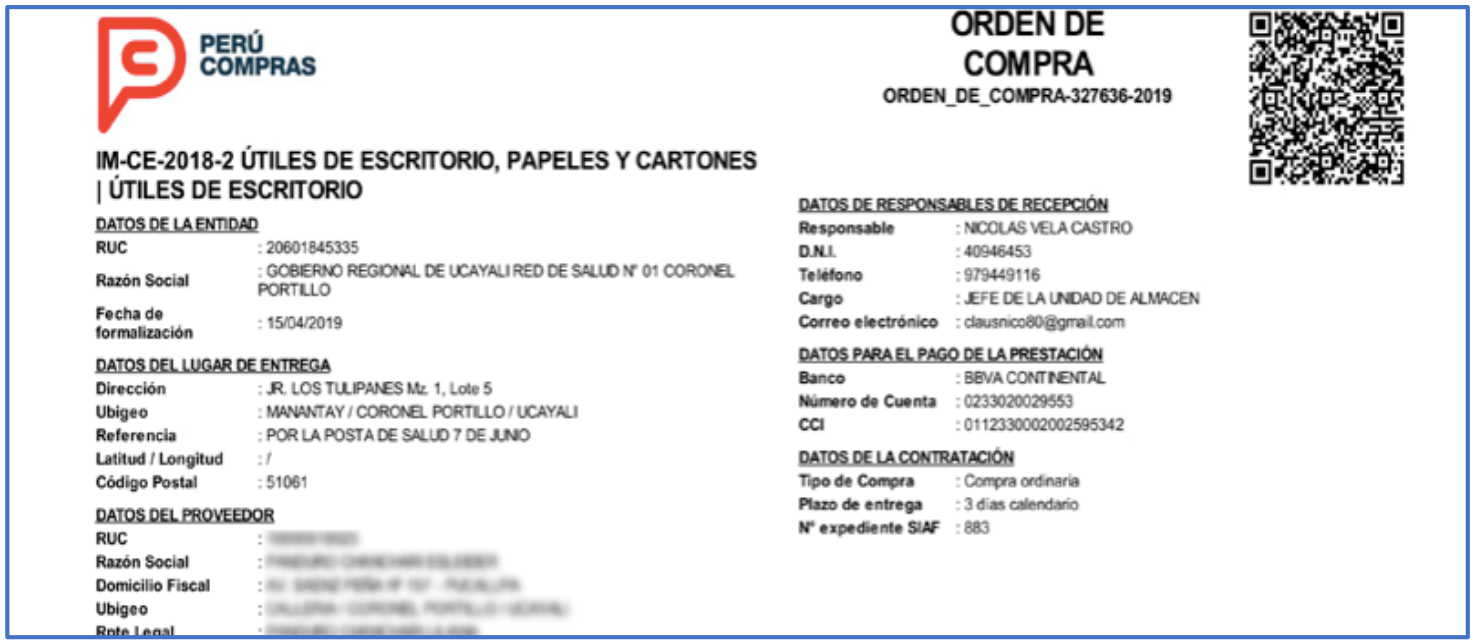
As a result, governments collect and copy information which is prone to errors and communication problems

Blockchain can be a cost-effective way to create a secure source of shared data to replace multiple, centralized information silos

Peru - Procurement

In May 2019, Perú Compras, the government procurement agency announced that it will put its procurement on a permissioned blockchain.*

For each tender, the platform will function as a smart contract where the tender, the offers and all related operations will be registered in an immutable and verifiable manner. In addition, contract payments will be linked, via smart contract, to events that demonstrate the degree of contract implementation.



PERÚ COMPRAS

ORDEN DE COMPRA

ORDEN_DE_COMPRA-327636-2019

IM-CE-2018-2 ÚTILES DE ESCRITORIO, PAPELES Y CARTONES | ÚTILES DE ESCRITORIO

DATOS DE LA ENTIDAD

RUC	: 20601845335
Razón Social	: GOBIERNO REGIONAL DE UCAYALI RED DE SALUD N° 01 CORONEL PORTILLO
Fecha de formalización	: 15/04/2019

DATOS DEL LUGAR DE ENTREGA

Dirección	: JR. LOS TULIPANES Mz. 1, Lote 5
Ubigeo	: MANANTAY / CORONEL PORTILLO / UCAYALI
Referencia	: POR LA POSTA DE SALUD 7 DE JUNIO
Latitud / Longitud	: /
Código Postal	: 51061

DATOS DEL PROVEEDOR

RUC	: [redacted]
Razón Social	: [redacted]
Domicilio Fiscal	: [redacted]
Ubigeo	: [redacted]
Rpte Legal	: [redacted]

DATOS DE RESPONSABLES DE RECEPCIÓN

Responsable	: NICOLAS VELA CASTRO
D.N.I.	: 40946453
Teléfono	: 979449116
Cargo	: JEFE DE LA UNIDAD DE ALMACEN
Correo electrónico	: clausnico80@gmail.com

DATOS PARA EL PAGO DE LA PRESTACIÓN

Banco	: BBVA CONTINENTAL
Número de Cuenta	: 0233020029553
CCI	: 011233002002595342

DATOS DE LA CONTRATACIÓN

Tipo de Compra	: Compra ordinaria
Plazo de entrega	: 3 días calendario
N° expediente SIAF	: 883

* LAC-Chain, launched by the Inter-American Development Bank and the initiative will collaborate with **Stamping.io**, a platform for certifying the traceability of goods https://observatorioblockchain.com/everis-entre-las-empresas-elegidas-por-el-bid-para-combatir-la-corrupcion-en-peru-con-blockchain/

Critical Factor #1
Trust Must be Earned!

For Blockchain applications, Data quality is extremely important

So a great deal of attention must be given to the process of adding data as well as the establishment of any initial baseline data

Otherwise,

Garbage in, Garbage forever!

Blockchain Data Quality

Remember:

While blockchains may be immutable and very transparent (you can see everything that was written and which "address" outside the blockchain made the change.

The correctness of blockchain data depends upon the quality of the EXTERNAL process(es) which decide what data will be written to the blockchain

So do not believe it, if someone says, "This data is true because it is on a blockchain"!

The truth is that, "This is the data that was written on the blockchain at time X" – even if that data was incorrect.

In Government Blockchain Applications,

Data Quality is a HUMAN RIGHTS ISSUE

Because data in a blockchain may decide what a citizen

- Legally owns
- The services and benefits they are entitled to
- The profesional activities they can undertake
- etc

Critical Factors/Hurdles 1

- Ensuring legal recognition of fully digitized contracts, both domestically and internationally
- Designing an effective digital twin (ID) for goods and transactions (i.e. how to represent physical goods on a blockchain network)
- Designing processes so that the “transactions” (events) recorded for digital twins reflect the information needed for decision making

Critical Factors/Hurdles 2

- Selecting a blockchain network to match an application's needs (security, speed, types of nodes, participation of nodes, etc.)
- For smart contracts: identifying decision points, decision criteria and exception handling (the 20% requiring 80% of the effort)
- Interoperability between blockchain networks. Citizens and companies today may interact with, at most, one or two blockchains. In 5-10 years they may be interacting with 15 or 20 blockchain networks – so they will need to be able to exchange information

Critical Factors/Hurdles 3

- **Scaling up, i.e. how to ensure that all participants register transactions and have the ability to do so.**
- **Identifying external data sources and developing consistent and secure data linkages**
- **Ensuring the quality of data, a critical point given the inability to change data entries in blockchain networks**

Critical Factors/Hurdles 4

- **Integrating blockchain solutions into legacy systems**
- **Resolving interoperability problems between multiple software systems using different technologies**
- **Obtaining a critical mass of users - which may require getting competitors to participate in <u>“competitive cooperation” models</u>**

Governments provide services that allow their citizens to fulfill their human potential

Therefore
the design and implementation of effective and efficient services is much more than just a question of making the best use of taxes

So it is important that developing countries have the tools available to implement blockchain in public services

Including open-source, free standards

Failing to ensure this will not just widen the information technology gap

It will widen the gap between developed and developing countries in all areas of human development

It is an opportunity to create a better future for them

Thank you!

Virginia Cram-Martos

www.triangularity.net