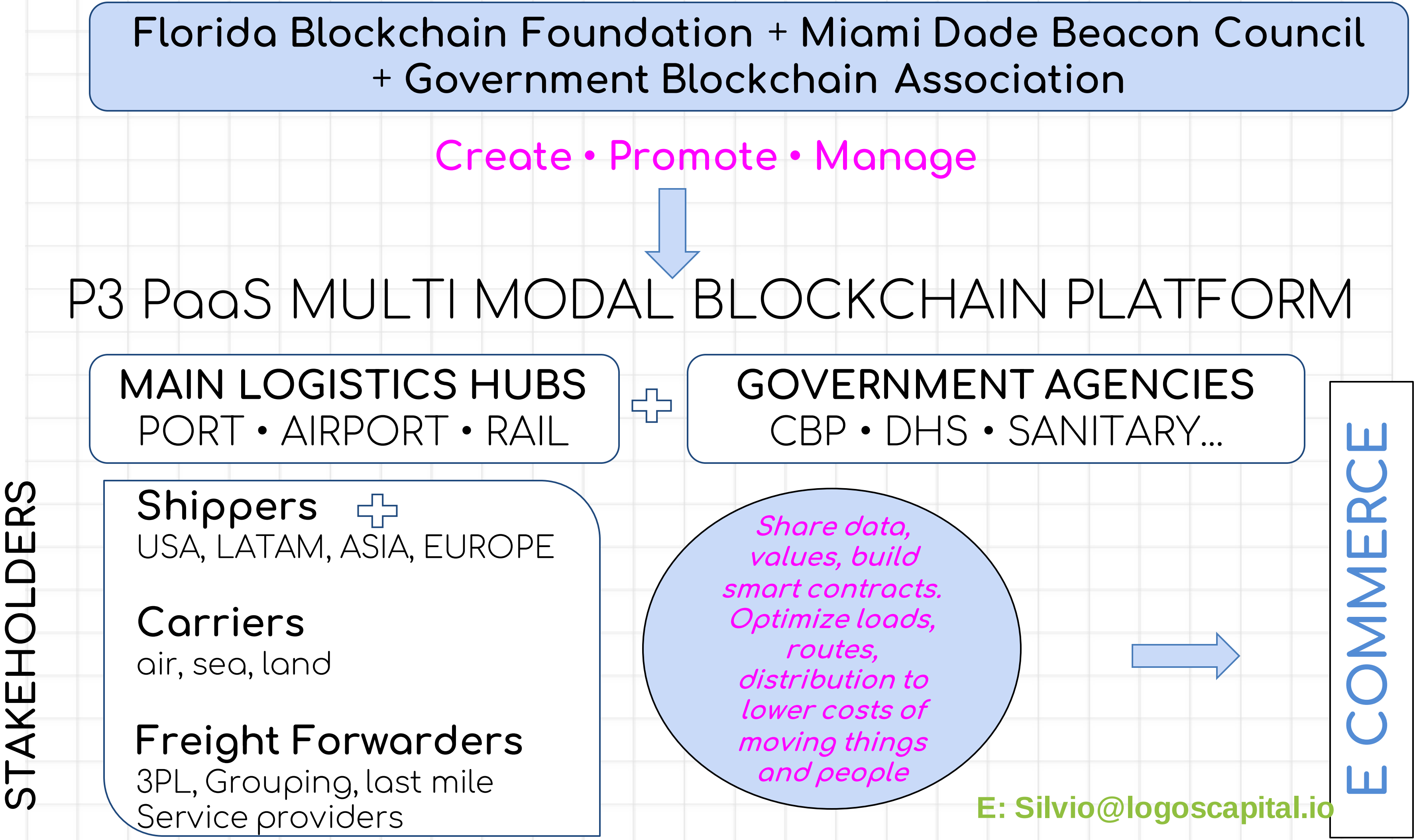
Blockchain Governance
+ Security Privacy Concerns

Airport Cooperative Research Program (ACRP)

By: Silvio Frank Pupo
E: Silvio@logoscapital.io

LOGOS CAPITAL



Florida Blockchain Foundation + Miami Dade Beacon Council + Government Blockchain Association

Create • Promote • Manage

P3 PaaS MULTI MODAL BLOCKCHAIN PLATFORM

MAIN LOGISTICS HUBS
PORT • AIRPORT • RAIL

+

GOVERNMENT AGENCIES
CBP • DHS • SANITARY...

STAKEHOLDERS

Shippers +
USA, LATAM, ASIA, EUROPE

Carriers
air, sea, land

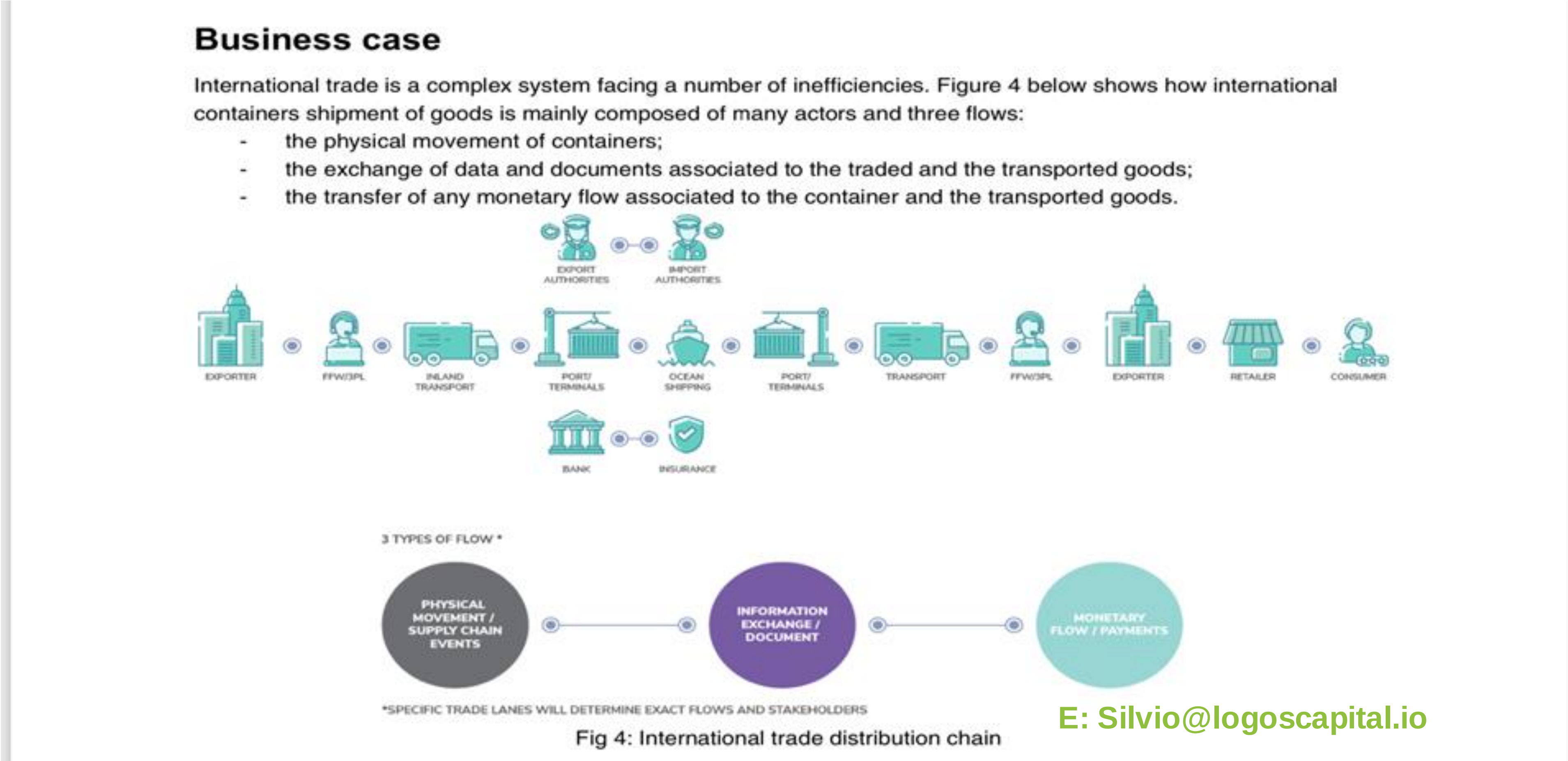
Freight Forwarders
3PL, Grouping, last mile
Service providers

Share data, values, build smart contracts. Optimize loads, routes, distribution to lower costs of moving things and people

E COMMERCE

E: Silvio@logoscapital.io

Business Case: Multimodal Miami



Business case

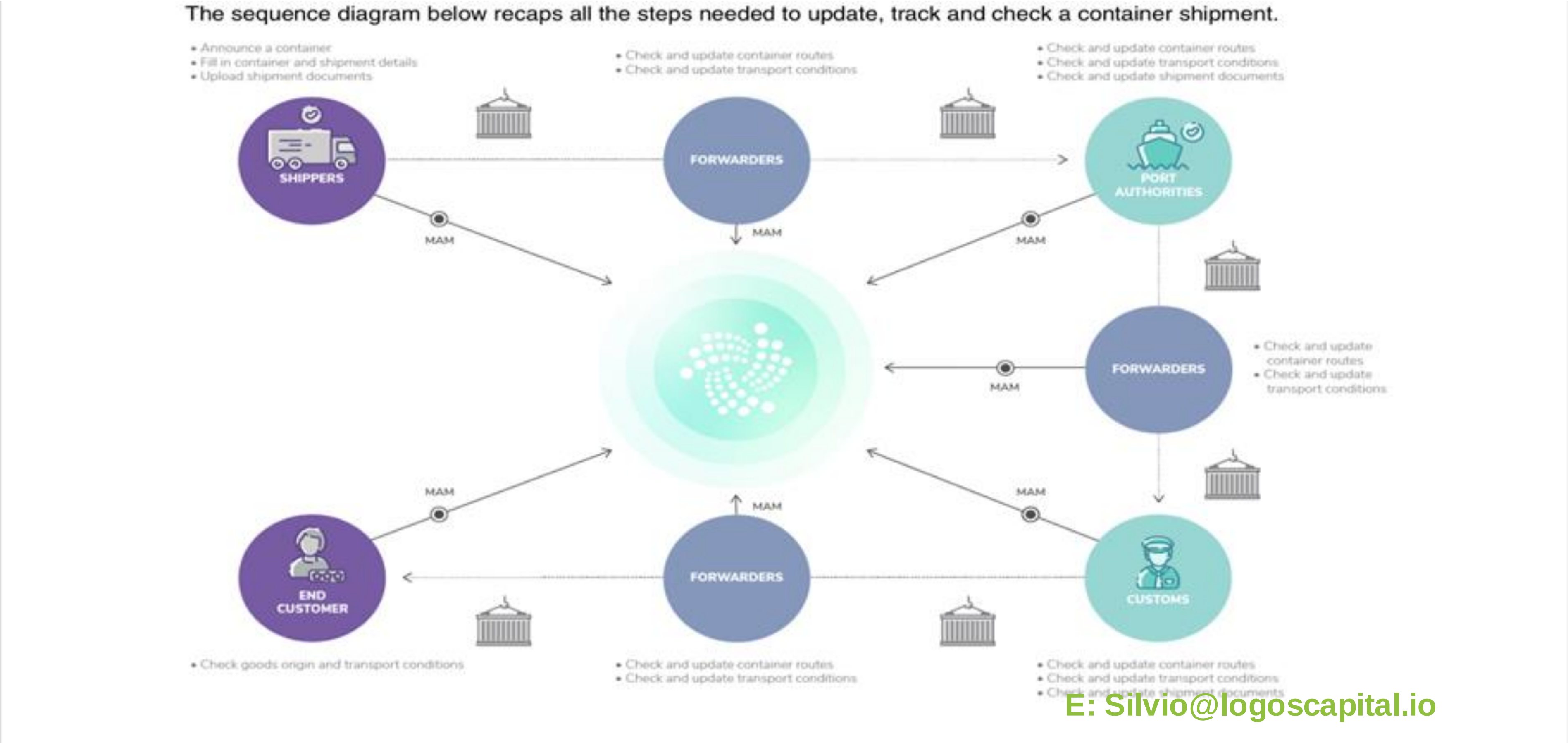
International trade is a complex system facing a number of inefficiencies. Figure 4 below shows how international containers shipment of goods is mainly composed of many actors and three flows:

- the physical movement of containers;
- the exchange of data and documents associated to the traded and the transported goods;
- the transfer of any monetary flow associated to the container and the transported goods.

Fig 4: International trade distribution chain

E: Silvio@logoscapital.io

Tracking a Shipping Container



The sequence diagram below recaps all the steps needed to update, track and check a container shipment.

- Announce a container
- Fill in container and shipment details
- Upload shipment documents

- Check and update container routes
- Check and update transport conditions

- Check and update container routes
- Check and update transport conditions
- Check and update shipment documents

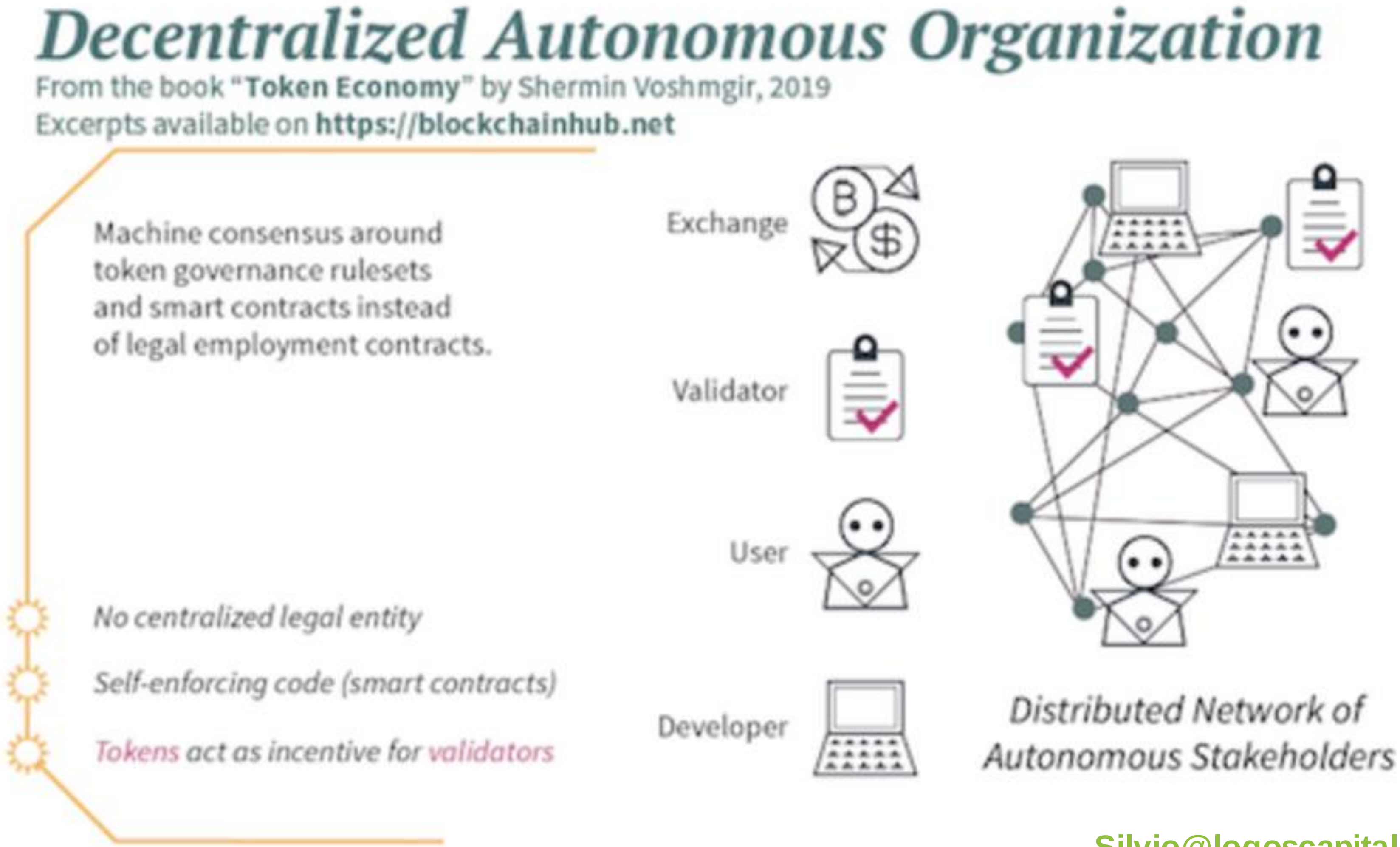
- Check and update container routes
- Check and update transport conditions

- Check goods origin and transport conditions

- Check and update container routes
- Check and update transport conditions

- Check and update container routes
- Check and update transport conditions
- Check and update shipment documents

E: Silvio@logoscapital.io



Decentralized Autonomous Organization

From the book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Machine consensus around token governance rulesets and smart contracts instead of legal employment contracts.

No centralized legal entity

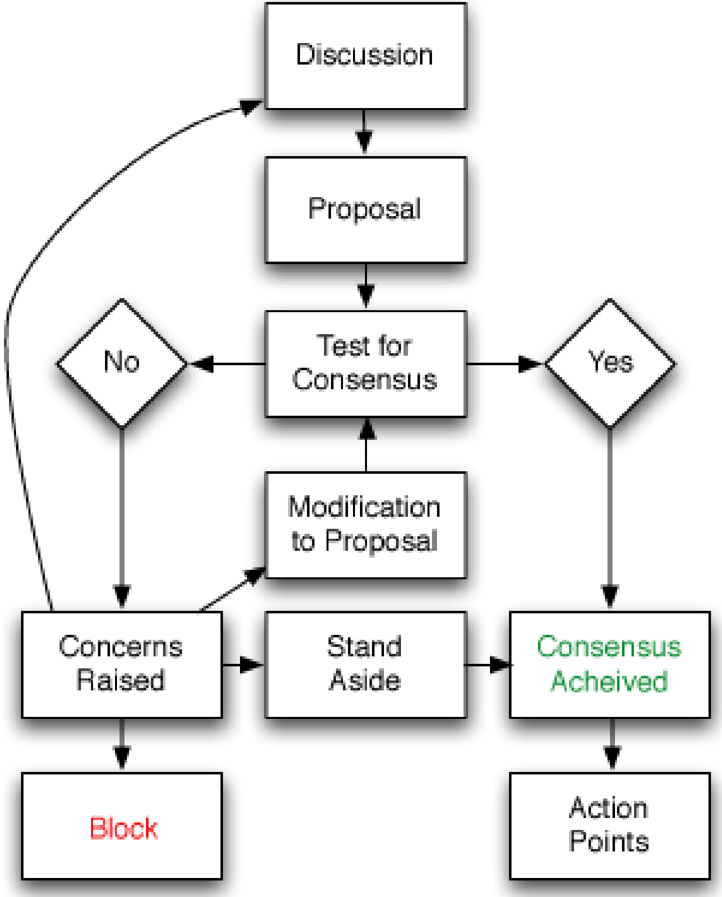
Self-enforcing code (smart contracts)

Tokens act as incentive for validators

Distributed Network of Autonomous Stakeholders

Silvio@logoscapital.io

Consensus: Group decision-making process for all



E: Silvio@logoscapital.io

"GAO"

Many people ask if the Government Blockchain Association (GBA) is just a theory or is it even possible?

Traditional Association Governance The GBA has established a set of GBA Bylaws that are designed to make the GBA a member-driven organization. GBA is led on a day-to-day basis by operation staff, but is under the oversight of a Board of Directors.

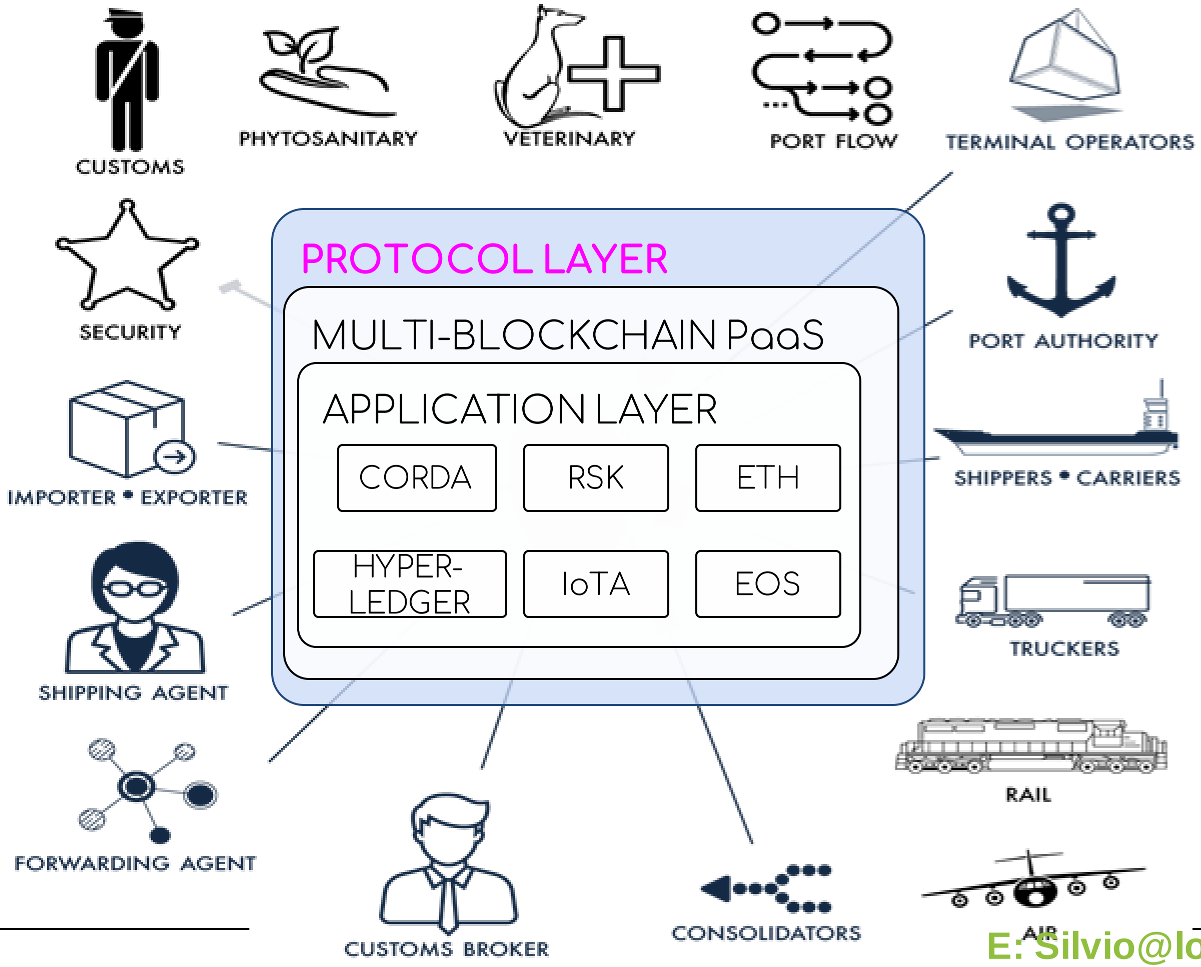
Distributed Autonomous Governance The GBA Working Group are beginning the journey towards distributed autonomous governance as a proof of concept. If it can be proven at a GBA Working Group and GBA Chapter Level, we can consider implementing these concepts and principals at regional, national, and global levels in the association.

GBA Governance - DAO Working Group The first working groups to explore the usage of these principles and models will be the GBA Governance Working Group. It is led by Max Gravitt, Founder of Digital Scarcity.

E: Silvio@logoscapital.io

THE
LAO

PLATFORM END-USERS



PROTOCOL LAYER

MULTI-BLOCKCHAIN PaaS

APPLICATION LAYER

CORDA

RSK

ETH

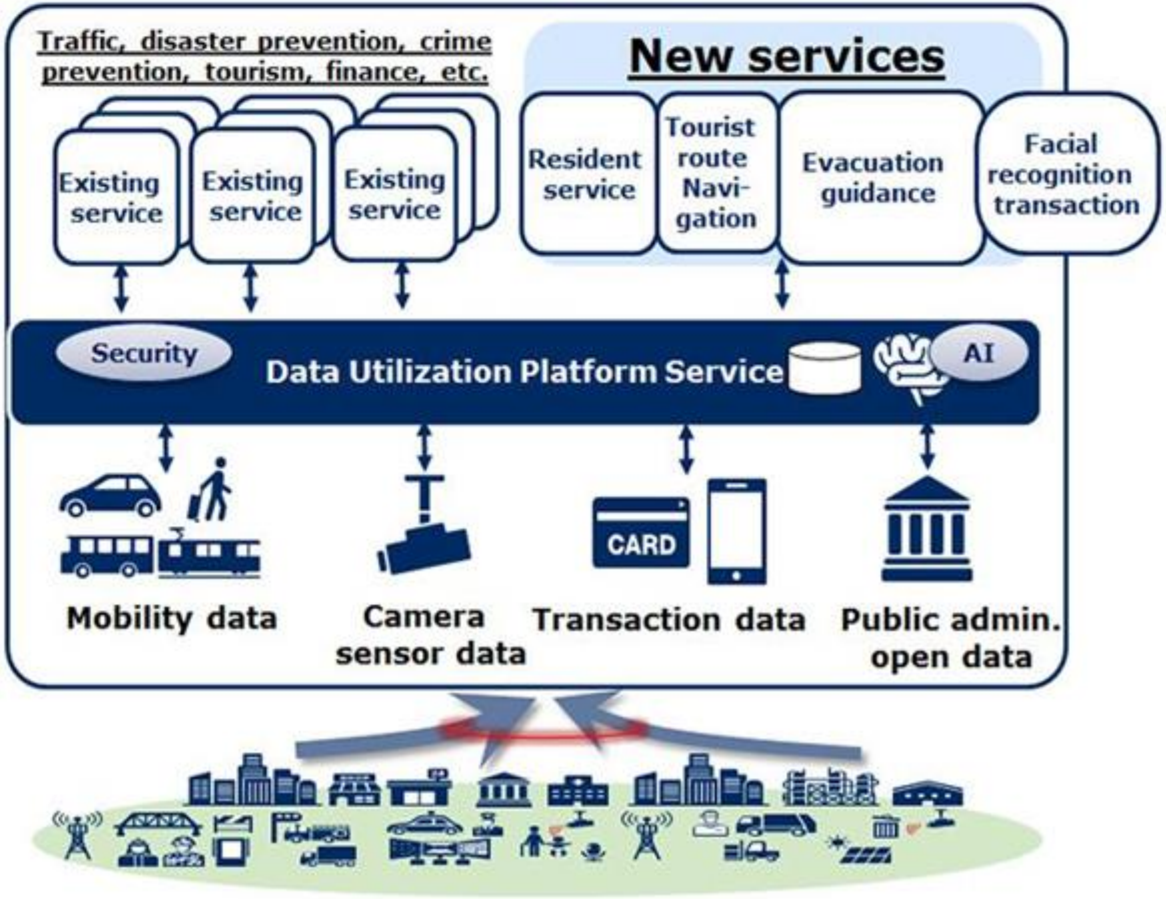
HYPER-LEDGER

IoTA

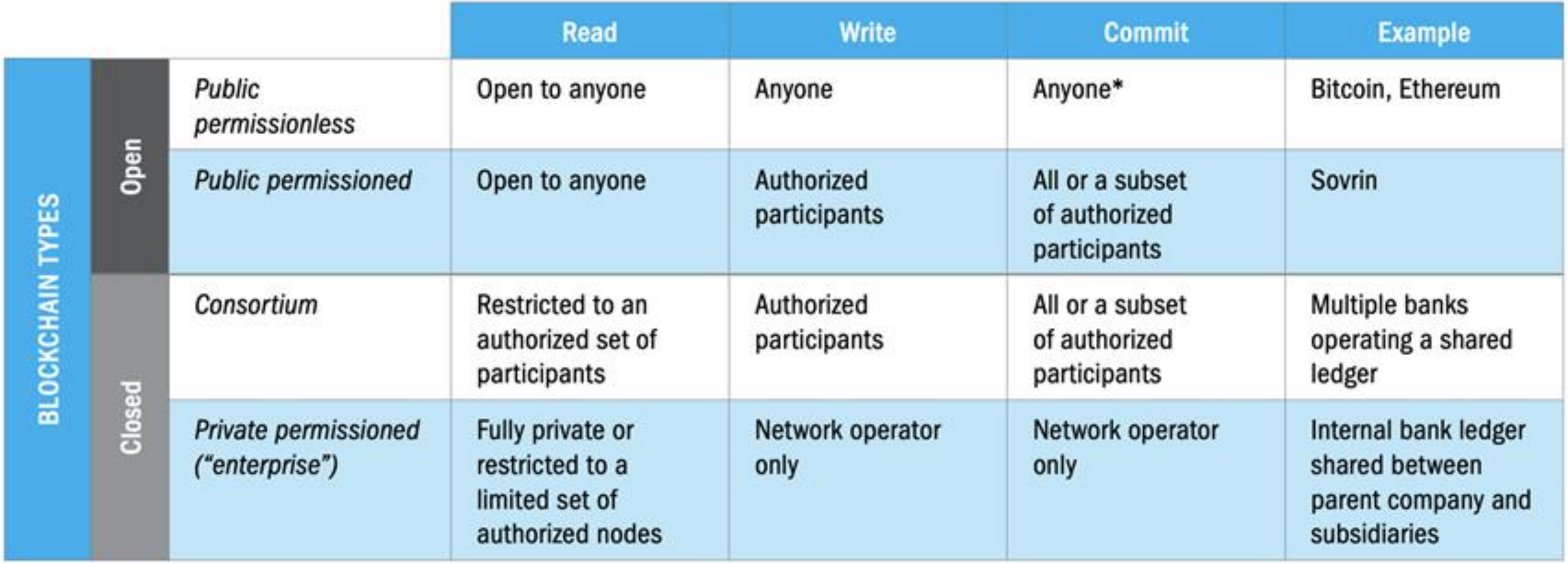
EOS

E: Silvio@logoscapital.io

Sample Data Utilization Platform



Comparing “open” versus “closed” protocols



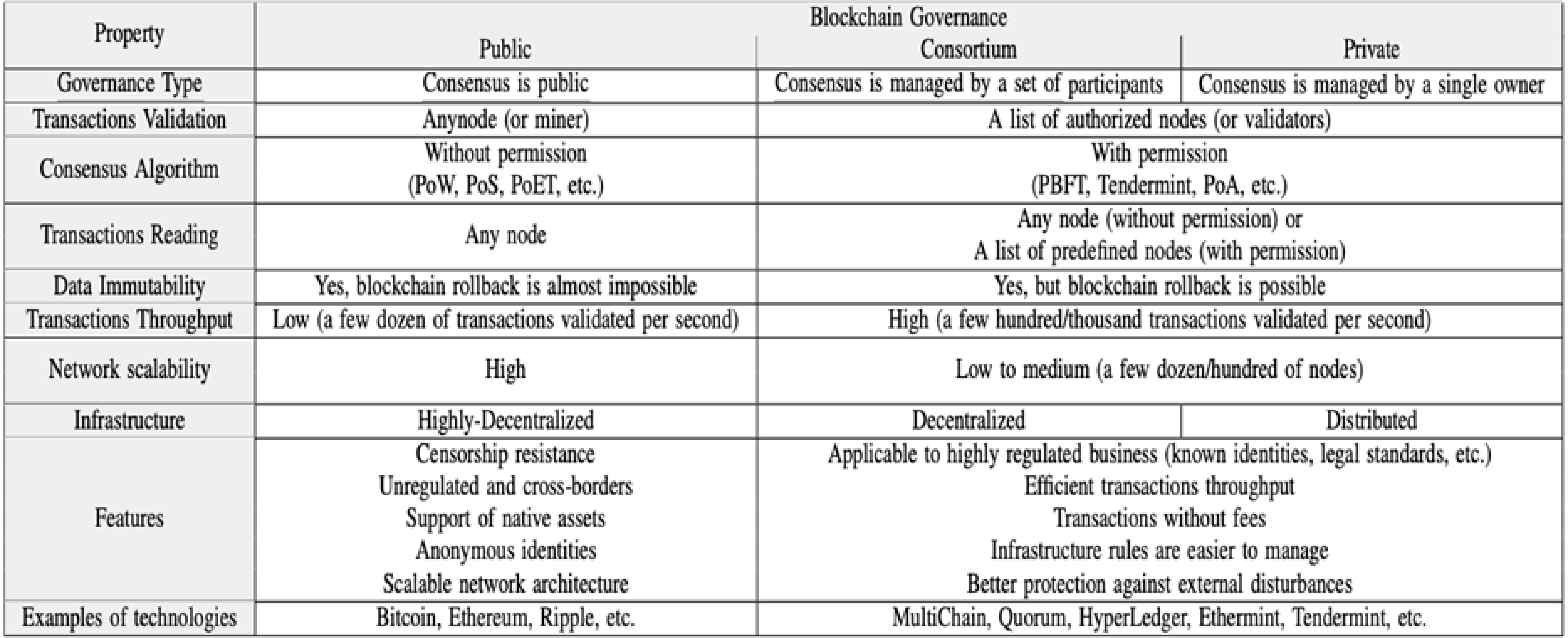
			Read	Write	Commit	Example
BLOCKCHAIN TYPES	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorized participants	All or a subset of authorized participants	Sovrin
	Closed	*Consortium*	Restricted to an authorized set of participants	Authorized participants	All or a subset of authorized participants	Multiple banks operating a shared ledger
		Private permissioned (“enterprise”)	Fully private or restricted to a limited set of authorized nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

*Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model)

FIGURE 1 **Main types of blockchains segmented by permission model**

Source: Hileman, Garrick and Michel Rauchs. 2017. “Global Blockchain Benchmarking Study.” Cambridge Centre for Alternative Finance.

E: Silvio@logoscapital.io



Property	Blockchain Governance		
	Public	Consortium	Private
Governance Type	Consensus is public	Consensus is managed by a set of participants	Consensus is managed by a single owner
Transactions Validation	Anynode (or miner)	A list of authorized nodes (or validators)	
Consensus Algorithm	Without permission (PoW, PoS, PoET, etc.)	With permission (PBFT, Tendermint, PoA, etc.)	
Transactions Reading	Any node	Any node (without permission) or A list of predefined nodes (with permission)	
Data Immutability	Yes, blockchain rollback is almost impossible	Yes, but blockchain rollback is possible	
Transactions Throughput	Low (a few dozen of transactions validated per second)	High (a few hundred/thousand transactions validated per second)	
Network scalability	High	Low to medium (a few dozen/hundred of nodes)	
Infrastructure	Highly-Decentralized	Decentralized	Distributed
Features	Censorship resistance Unregulated and cross-borders Support of native assets Anonymous identities Scalable network architecture	Applicable to highly regulated business (known identities, legal standards, etc.) Efficient transactions throughput Transactions without fees Infrastructure rules are easier to manage Better protection against external disturbances	
Examples of technologies	Bitcoin, Ethereum, Ripple, etc.	MultiChain, Quorum, HyperLedger, Ethermint, Tendermint, etc.	

E: Silvio@logoscapital.io

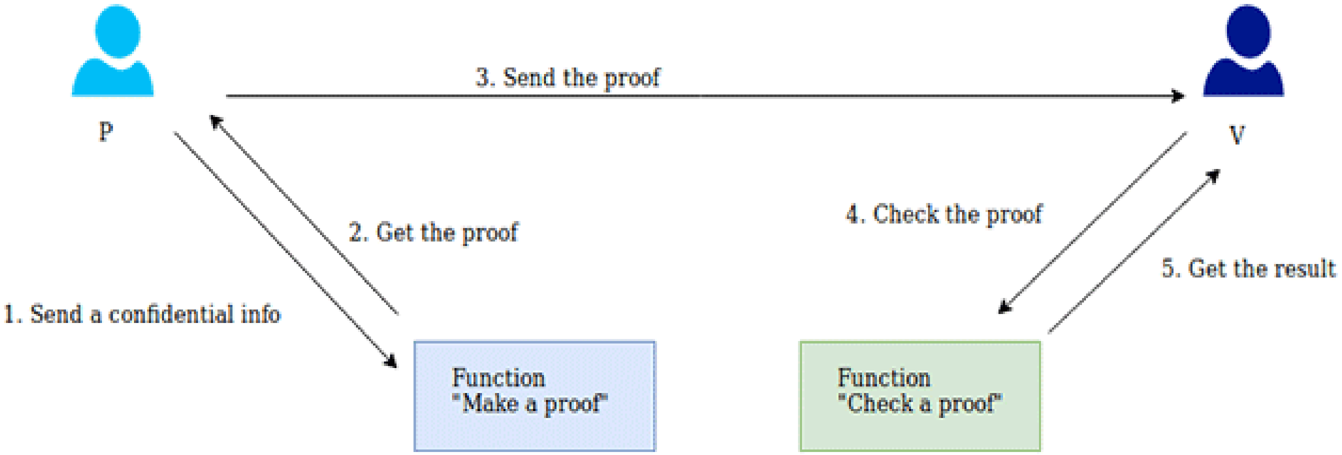
Blockchain and privacy protection

Private and public keys

Peer-to-peer network

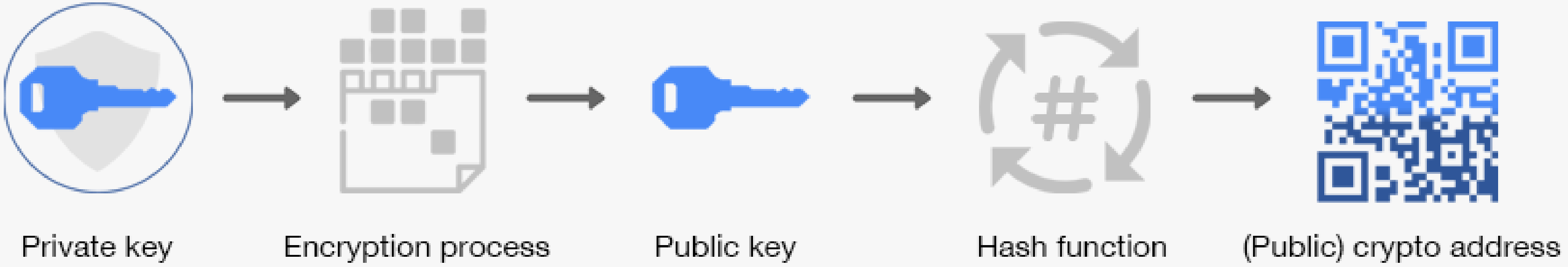
Zero-knowledge proofs

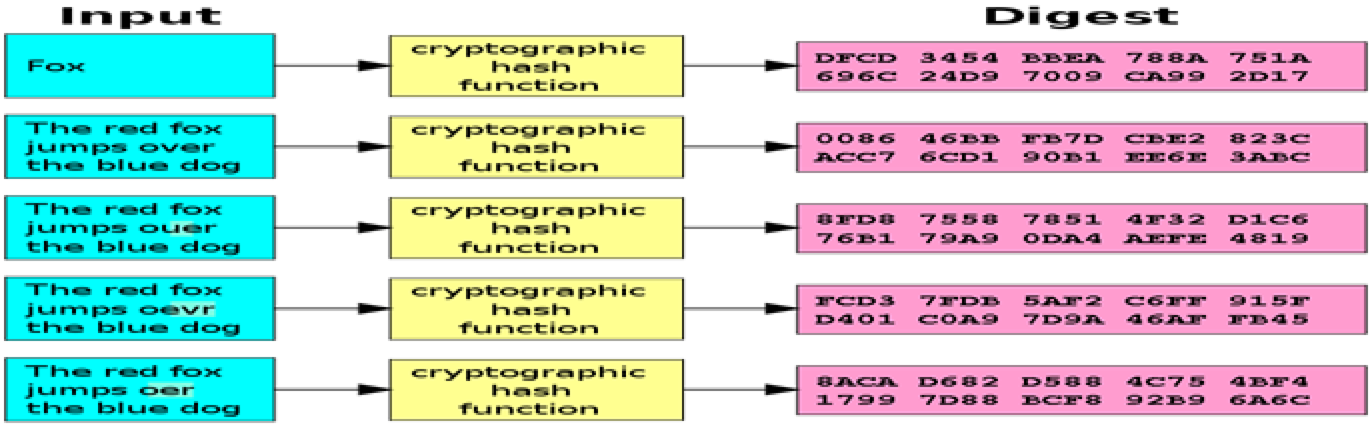
ZKP background

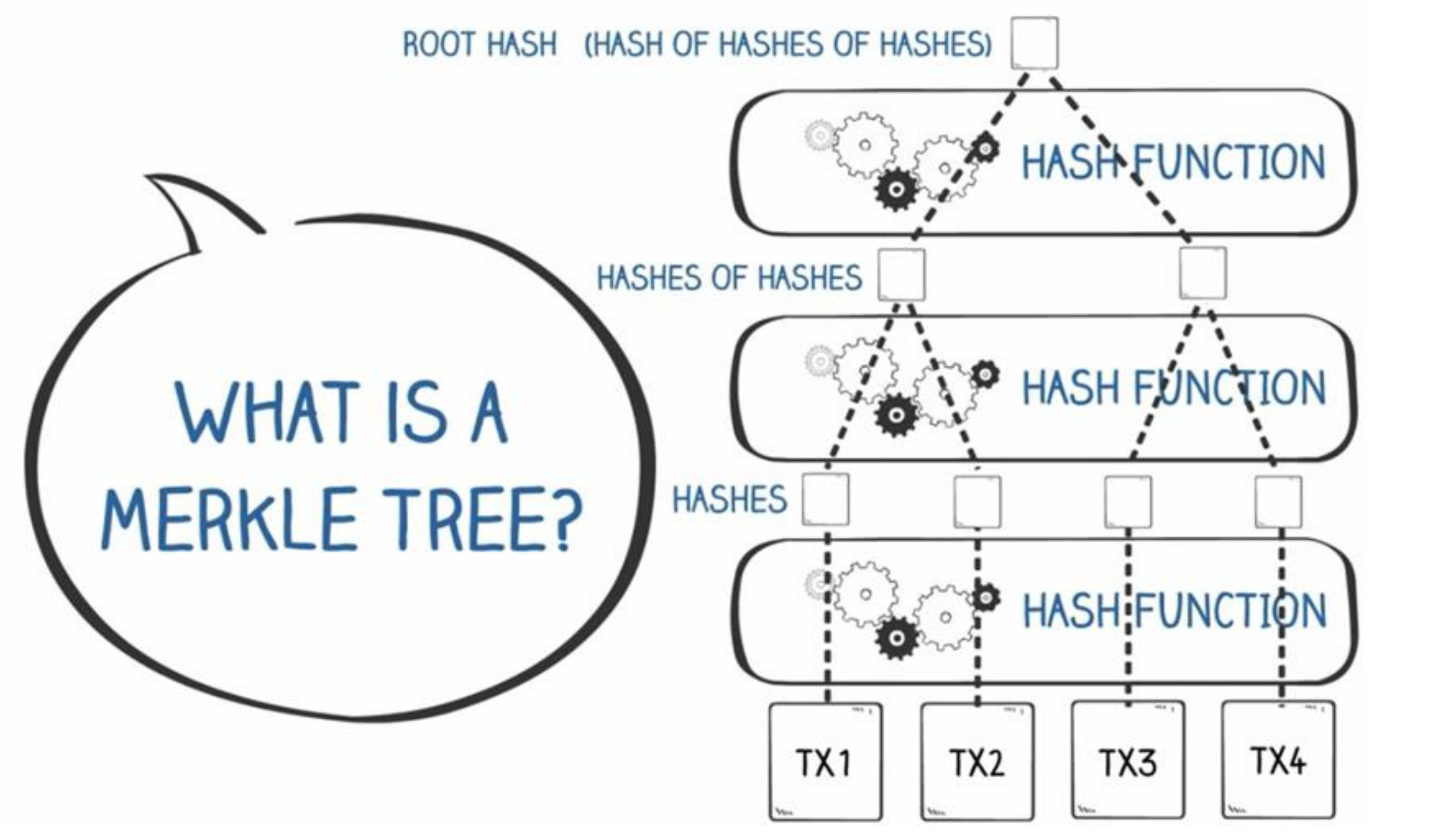


E: Silvio@logoscapital.io

From Private Key to Public Address




Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C



E: Silvio@logoscapital.io

Legality of blockchain and privacy

GDPR: Because identities on a blockchain are associated with an individual's public and private keys, this may fall under the categ ory of personal data because public and private keys enable pseudonymity and are not necessarily connected to an identity.[14] A key part of the GDPR lies in a citizen's right to be forgotten, or data erasure.[14] The GDPR allows individuals to request that data associated with them to be erased if it is no longer relevant.[14] Due to the blockchain's nature of immutability, potential complications if an individual who made transactions on the blockch ain requests their data to be deleted exist.[14] Once a block is verified on the blockchain, it is impossible to delete it.[8]

Blockchain Alliance: Because virtual currencies and the blockchain's protection of identity has proved to be a hub for criminal purchases and activity, FBI and Justice Department created Blockchain Alliance.[13] This team aims to identify and enforce legal restrictions on the blockchain to combat criminal activities through open dialogue on a private-public forum.[13] This allows law enforcers to fight the illegal exploitation of the technology.[13] Examples of criminal activity on the blockchain include hacking cryptocurrency wallets and stealing funds.[2] Because user identities are not tied to public addresses, it is difficult to locate and identify criminals.[2]

Fair information practices Blockchain has been acknowledged as a way to solve fair information practices, a set of principles relating to privacy practices and concerns for users.[5] Blockchain transactions allow users to control their data through private and public keys, allowing them to own it.[5] Third-party intermediaries are not allowed to misuse and obtain data.[5] If personal data are stored on the blockchain, owners of such data can control when and how a third party can access it. In blockchains, ledgers automatically include an audit trail that ensures transactions are accurate.[5]

E: Silvio@logoscapital.io

Concerns regarding blockchain privacy

Transparency: Although many[who?] advocate for the adoption of blockchain technology because it allows users to control their own data and exclude third parties, some[who?] believe certain characteristics of this technology infringe on user privacy.[16] Because blockchains are decentralized and allow any node to access transactions, events and actions of users are transparent.[16] Sceptics[who?] worry malicious users can trace public keys and addresses to specific users. If this was the case, a user's transaction histo ry would be accessible to anyone, resulting in what some[who?] consider to be a lack of privacy.[16]

Decentralization: Due to blockchain decentralized nature, a central authority is not checking for malicious users and attacks.[16] Users might be able to hack the system anonymously and escape.[16] Because public blockchains are not controlled by a third party, a false transaction enacted by a hacker who has a user's private key cannot be stopped.[2] Because blockchain ledgers are shared and immutable, it is impossible to reverse a malicious transaction.[2]

Private Keys: Private keys provide a way to prove ownership and control of cryptocurrency.[2] If one has access to another's private key, one can access and spend these funds.[2] Because private keys are crucial to accessing and protecting assets on the blockchain, users must store them safely.[2] Storing the private key on a computer, flash drive or telephone can pose potential security risks if the device is stolen or hacked.[2] If such a device is lost, the user no longer have access to the cryptocurrency.[2] Storing it on physical media, such as a piece of paper, also leaves the private key vulnerable to loss, theft or damage.[2]v

E: Silvio@logoscapital.io