Hogan Lovells

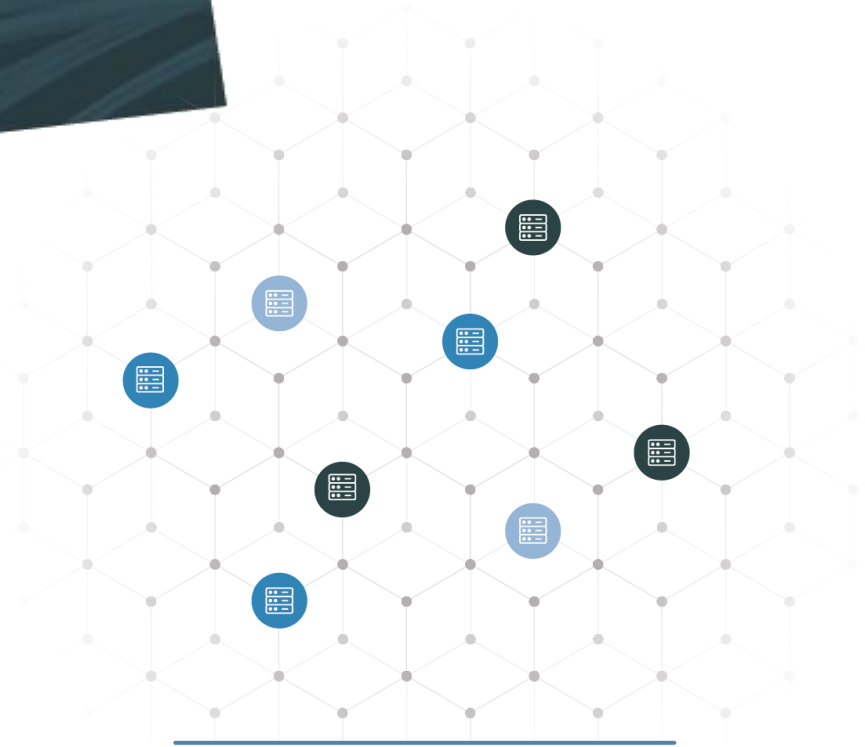
ParalympicsGB

OFFICIAL PARTNER

Regulatory Challenges Facing Cryptoassets

Centralised v decentralised

Centralised company

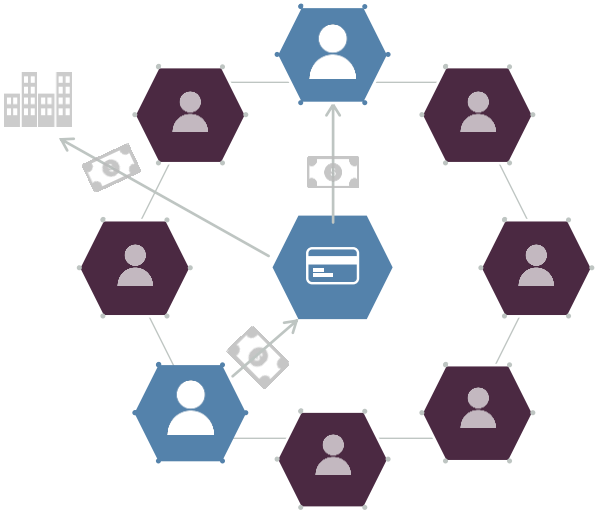


Decentralised company
(blockchain)

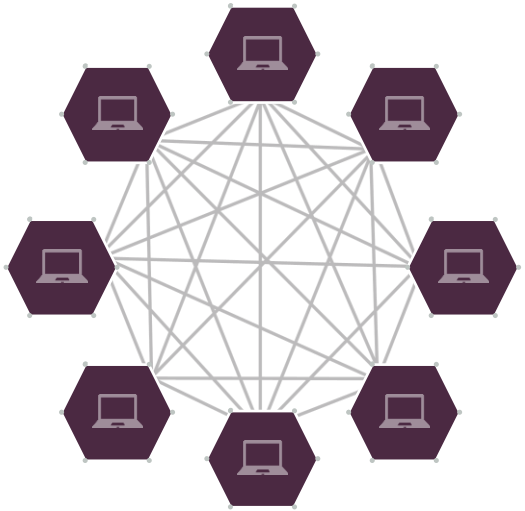
Distributed ledger

Instead of your bank having control over your account ledger, control of the ledger is decentralised and dispersed among multiple computers on the network.

Each computer holds a copy of the distributed ledger



Current payment systems require third-party intermediaries that often charge high processing fees…



… but peer-to-peer payment using a distributed ledger could allow for direct payment between individuals

Centralised v decentralised

Centralised company

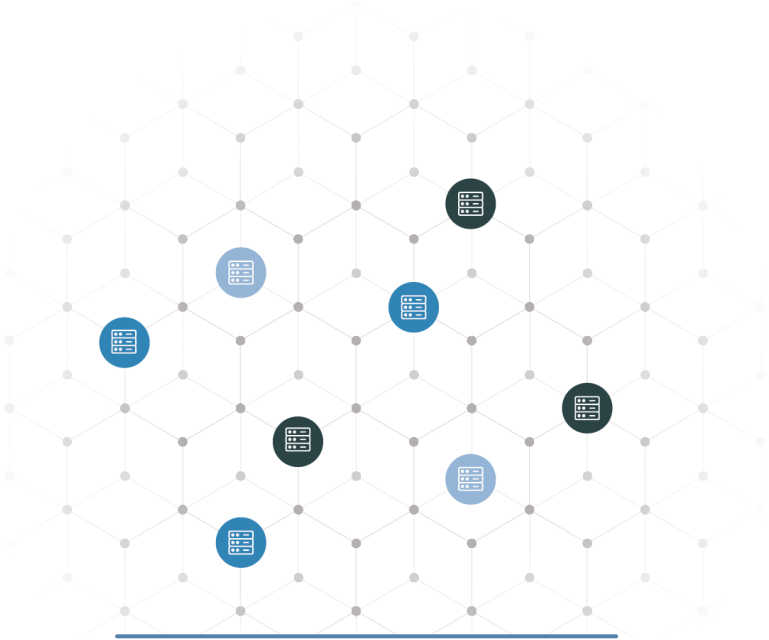
- Clear governance
- Single trusted party
- Easy to identify responsibility
- Regulatory certainty (possibly regulated depending on sector)

How blockchain works

Decentralised	*Cryptography*	*Distributed ledger*	*Consensus protocol*	*Immutability*
The network is decentralised, meaning that there is not a single governing authority or person, instead there is a network of nodes.	To protect the data, cryptography is used as a form of encryption.	Every node on the network has a copy of the ledger. Every transaction is therefore cross-checked across all ledgers and prevents data loss.	When a new transaction is made, every node on the network is asked to verify that this transaction is in line with the prior transactions recorded on their ledger.	Every block on the blockchain has a unique hash. Each block references the previous block. If someone were to tamper with a block in the chain, it would alter all subsequent blocks and would identify this as false.

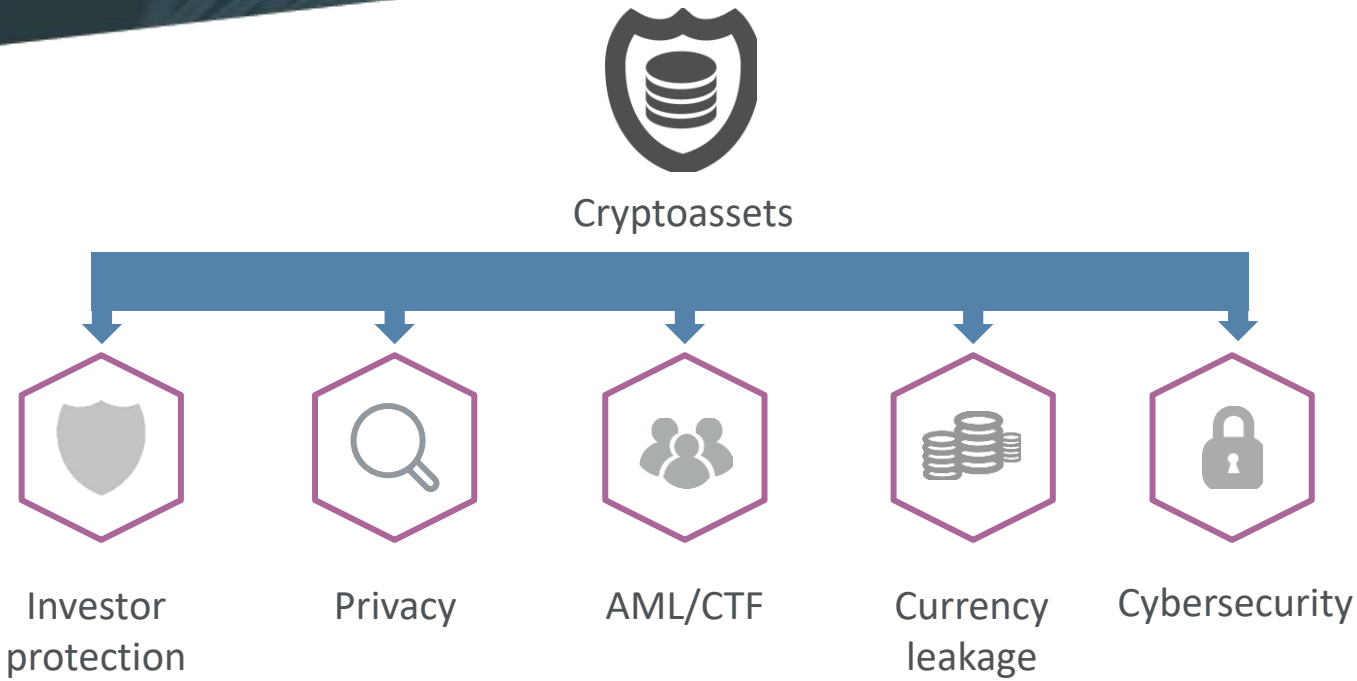
Centralised v decentralised

- Unclear governance
- Trustless
- Difficult to identify responsibility
- Legal uncertainty



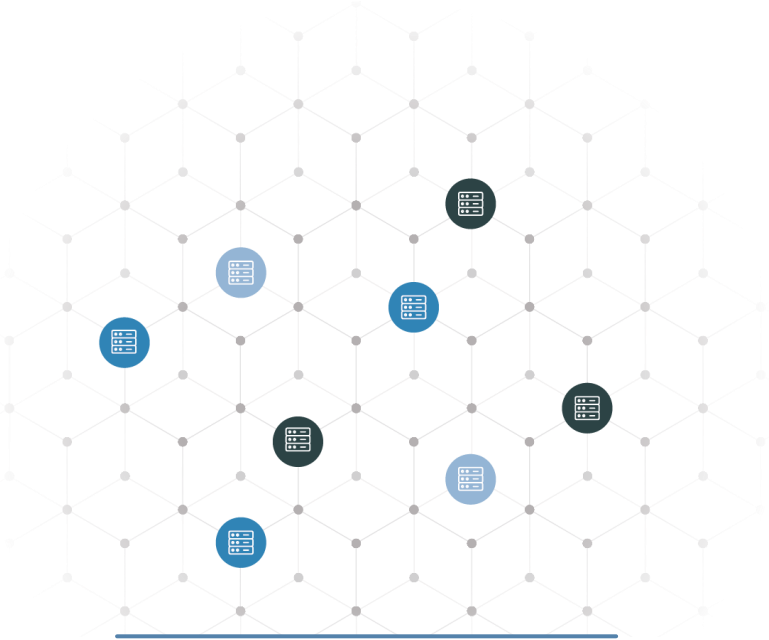
Decentralised company
(blockchain)

What are regulators worried about?



Investor protection

- Token categorisation
- Perimeter issues
- Decentralisation



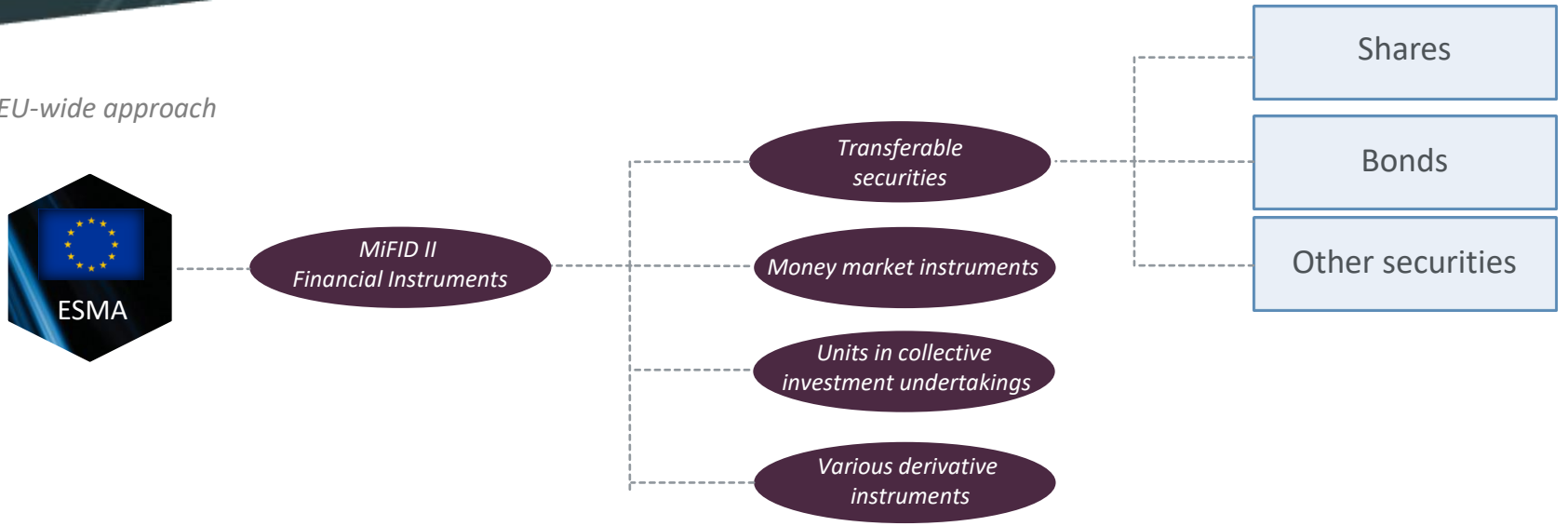
Decentralised company
(blockchain)

Tokens - categorisation

Payment token	Asset token	Consumer token
Akin to a traditional currency Used as a medium of exchange for any goods	Represents an underlying financial asset Analogous to traditional securities such as bonds, equities or derivatives	Gives the user ownership or coupon rights to a specific set of goods and/or services
E-money?	Regulated	Not regulated, but depends

Asset tokens

EU-wide approach



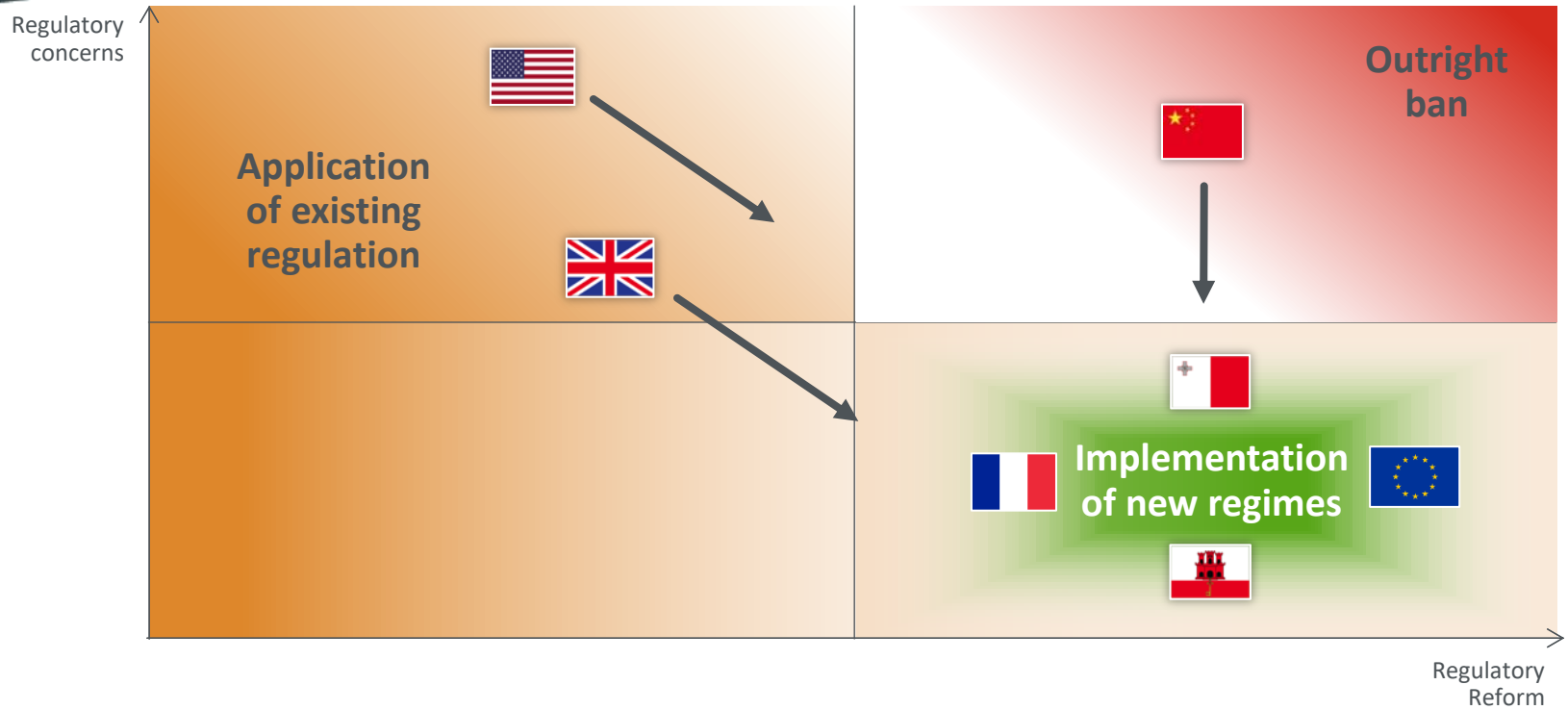
Payment tokens

EU approach

EMD2
E-money

- is electronically stored;
- has monetary value;
- represents a claim on the issuer;
- is issued on receipt of funds;
- is issued for the purpose of making payment transactions;
- is accepted by persons other than the issuer.

Perimeter issues



UK approach - FCA framework

Regulated tokens

Security tokens

- i.e. tokens satisfying definition of specified investments under RAO (excluding e-money)

E-money tokens

- i.e. tokens meeting definition of e-money under the EMRs

Unregulated tokens

Utility tokens

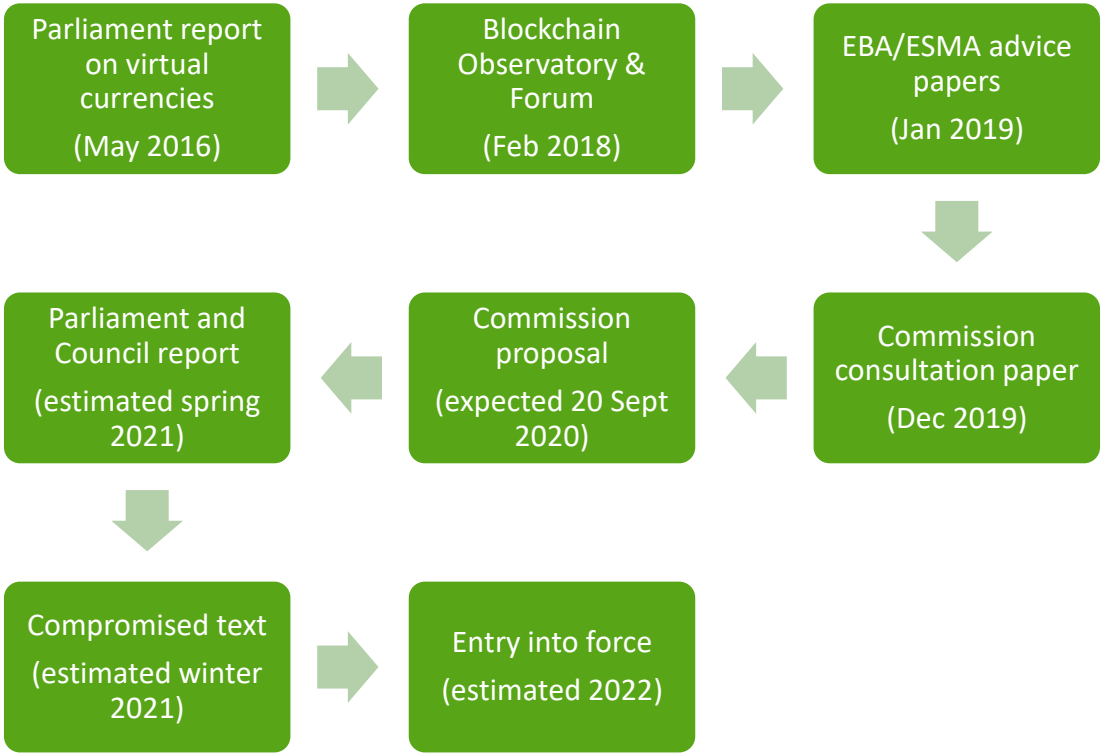
- i.e. tokens redeemable for access to a specific product or service (akin to vouchers)

Exchange tokens /cryptocurrencies

- i.e. designed primarily as a medium of exchange (e.g. bitcoin)

Starting point for analysis → What are its key characteristics? → How does it work?

The EU approach



Implementing new regimes

Gibraltar approach – Jan 2018

WHAT

- A framework built on ensuring adequate and accurate disclosure and adherence with AML/CFT

WHY

- "Creating legislation that will provide strong oversight and consumer protection without stifling the innovation"

IMPACT

- Thirteen firms have been granted licenses

Implementing new regimes

Malta approach – July 2018

WHAT

- Implemented three new pieces of legislation to bring cryptoassets into the regulated space

WHY

- Aim to be "blockchain island"

IMPACT

- Foreign crypto players set up operations in Malta
- Fourteen cryptoasset agents approved

Implementing new regimes

France approach – May 2019

WHAT

- A voluntary regime which token issuers can opt into to gain an AMF license

WHY

- "Ambition to make France an ICO capital"
- "We cannot regulate new technology with ancient regulation"

IMPACT

- Reignited conversation in Brussels to have a unified approach to cryptoassets
- Improved visibility of 'legitimate' projects

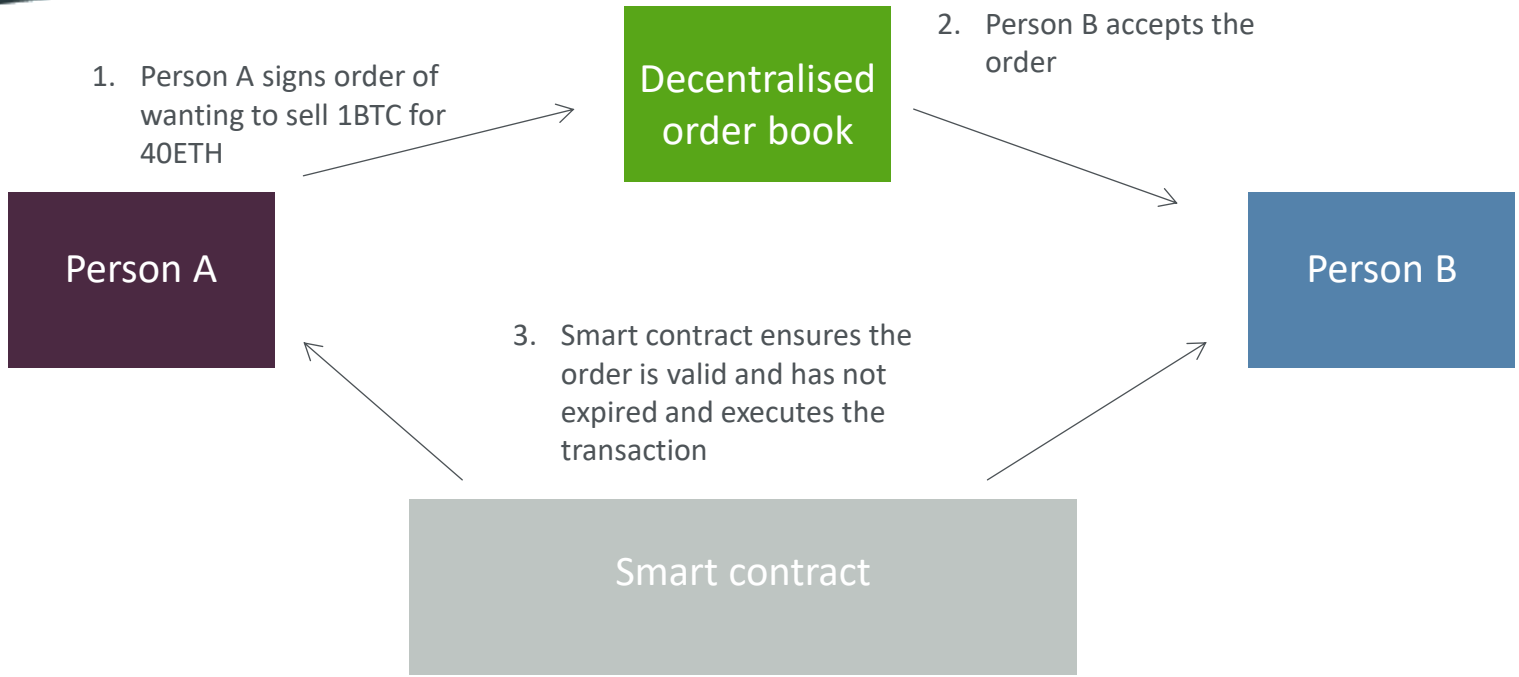
Decentralised finance

User Interface

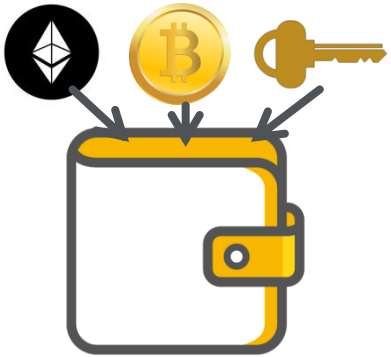
Application Layer

Blockchain infrastructure

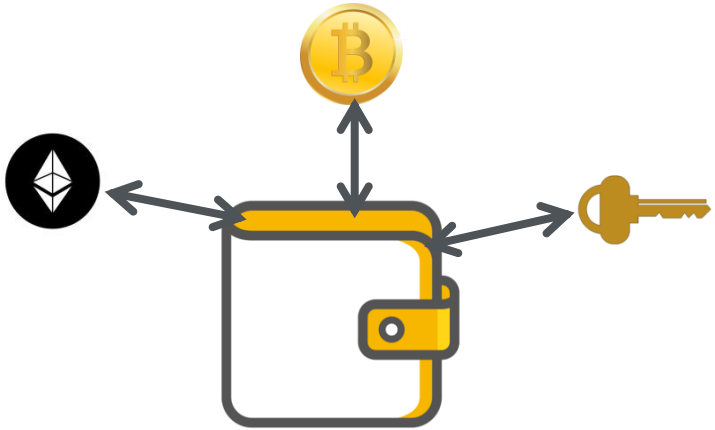
Decentralisation – exchanges



Decentralisation – non-custodial wallets



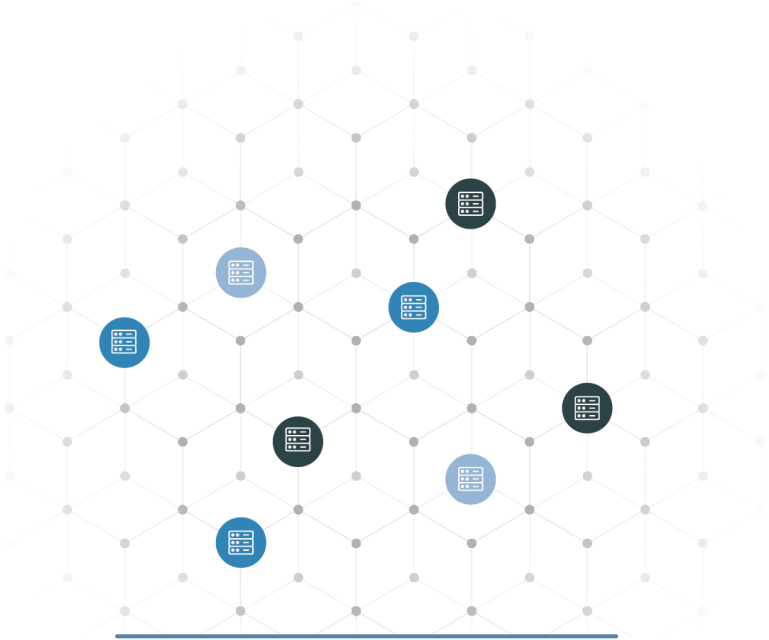
Custodial wallets



Non-custodial wallets

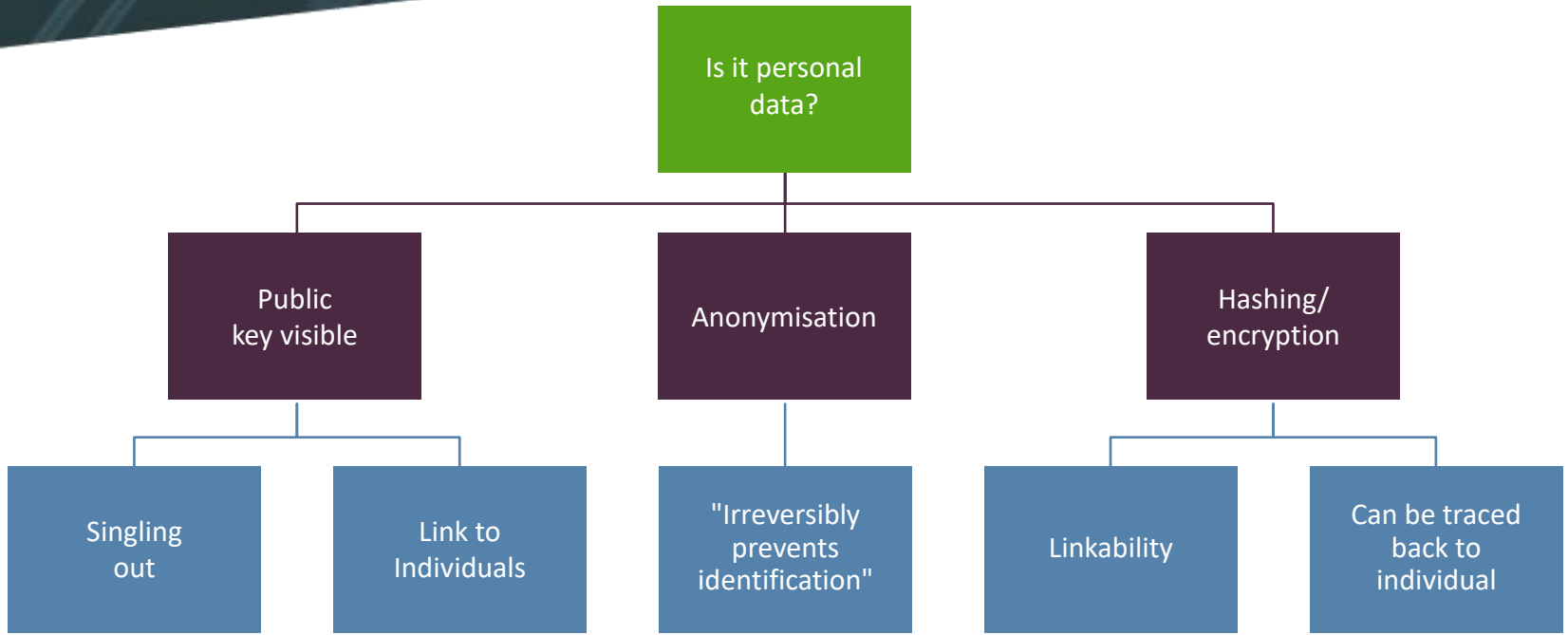
Privacy

- Is there personal data?
- Who is the controller?
- Has there been a transfer?
- Immutable data

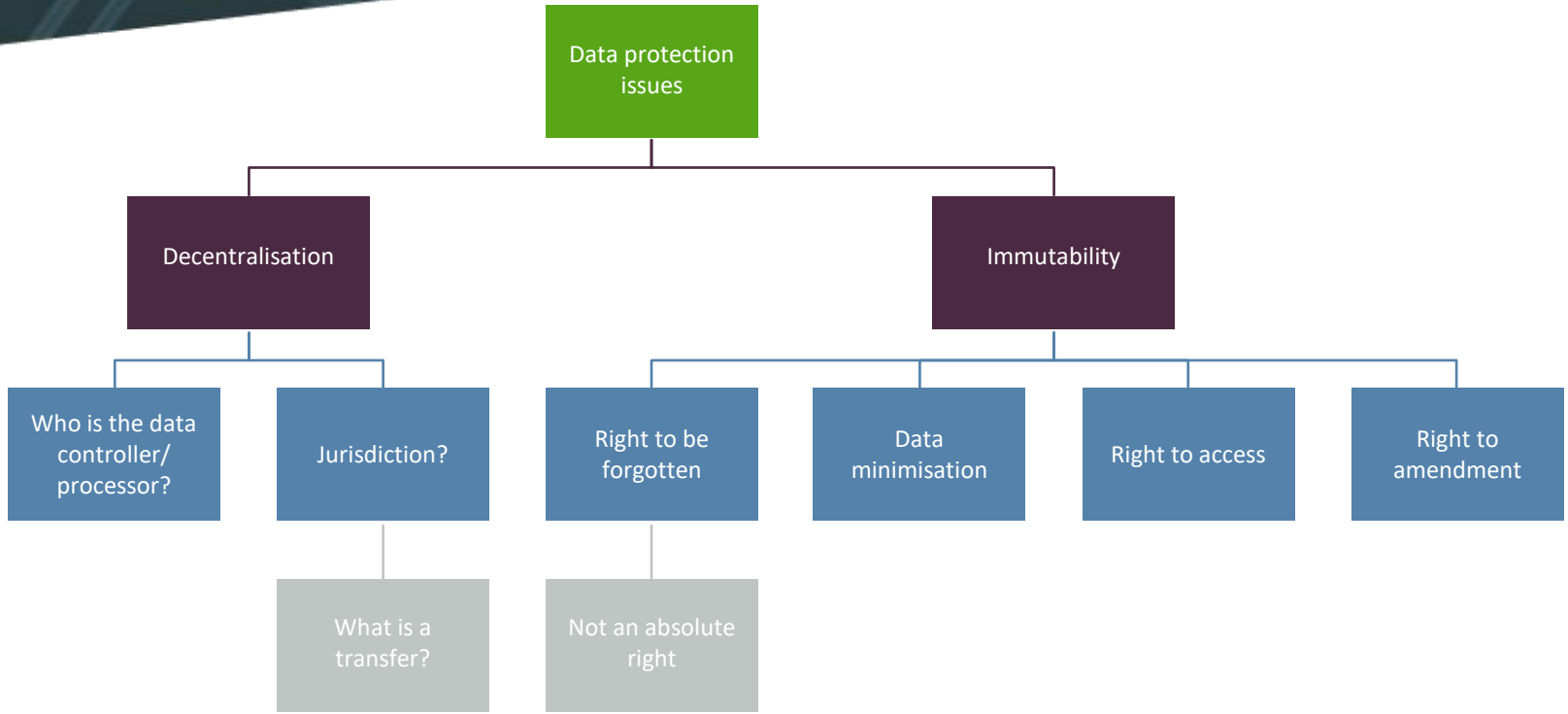


Decentralised company
(blockchain)

Key legal challenges
Privacy and data protection



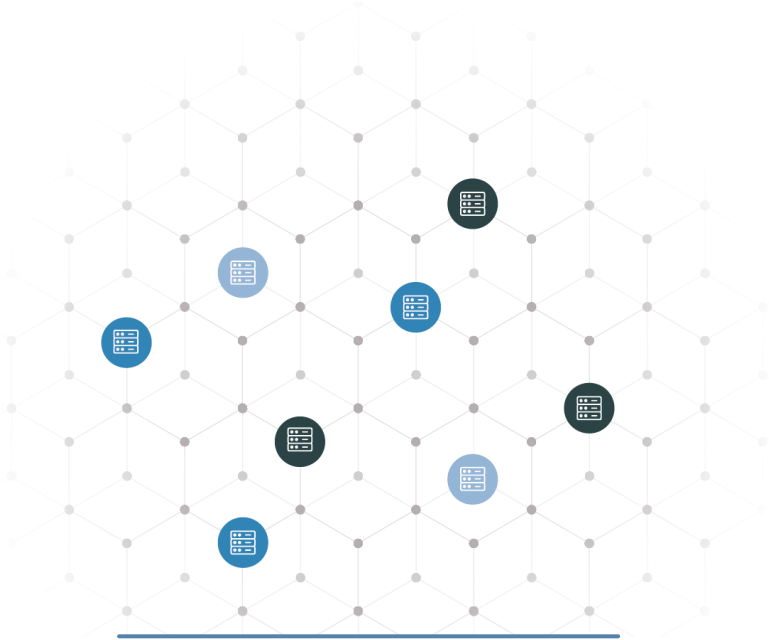
Key legal challenges
Privacy and data protection



AML

Custodial wallet providers

Cryptoasset exchanges



Decentralised company
(blockchain)

5AMLD

Implements the Financial Action Task Force guidelines on anti-money laundering – 5AMLD implements measures to bring transparency to cryptoasset transactions.

- Cryptoasset transactions can be anonymous
  - Concerns that this will be used to conceal financial transactions
- 5AMLD brings cryptoasset exchanges and custodian wallet providers within the scope of the money laundering directive
- Providers will have the responsibility to monitor transactions and verify customer IDs

5AMLD – cryptoasset exchanges

Activities pertaining to a cryptoasset exchange are:

- exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets;
- exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another; or
- operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.

AML – custodial wallet provider

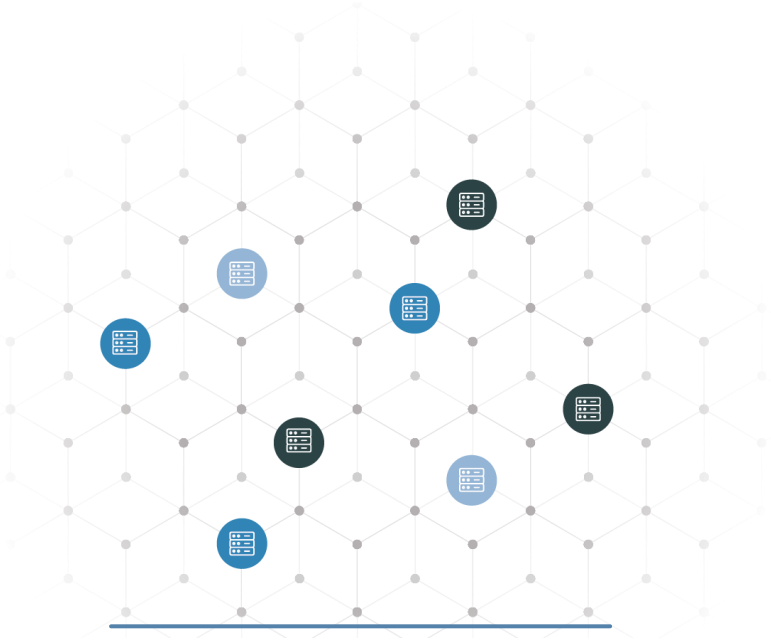
Activities pertaining to a custodian wallet provider are:

- Providing services to safeguard, or to safeguard and administer:
  - cryptoassets on behalf of its customers; or
  - private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets, when providing such services.

Currency leakage

Consumer protection

Monetary control



Decentralised company
(blockchain)

Stablecoins – consumer protection

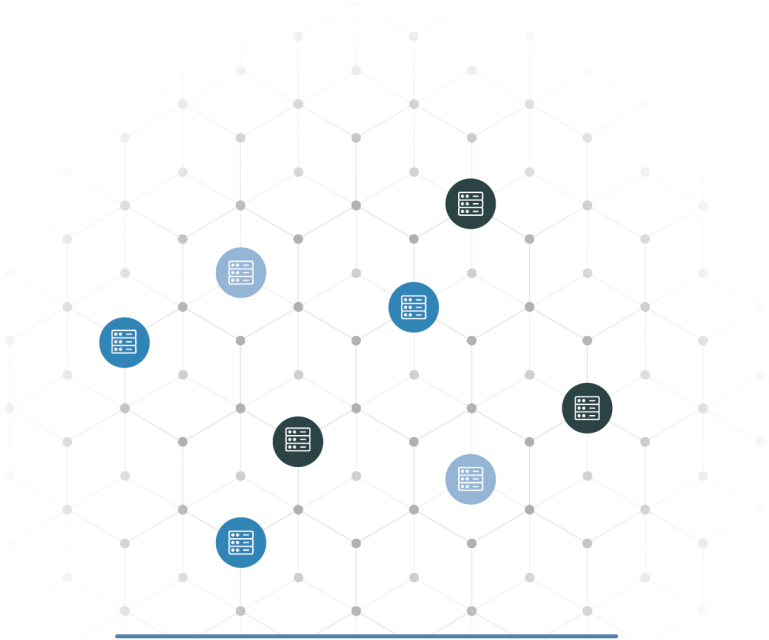
- Legal certainty
- Sound governance
- AML/CTF
- Safety, efficiency and integrity of payment system
- Cyber security and operational resilience
- Market integrity
- Data privacy

Stablecoins – monetary control

- Monetary policy
- Financial stability
- International monetary system
- Fair competition

Cybersecurity

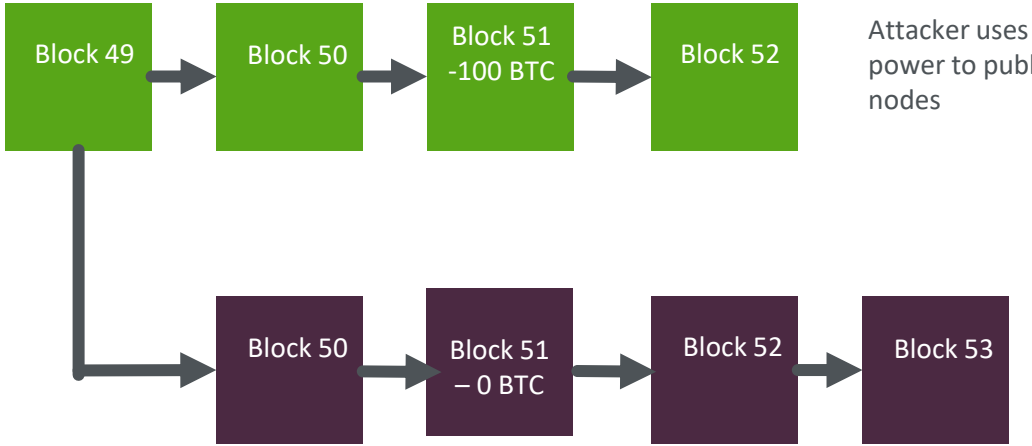
- Brute force attacks
- Double spending
- DDoS attacks
- Quantum computing



Decentralised company
(blockchain)

Brute force attacks

Honest nodes add blocks to the public blockchain



Attacker uses 51% of networks mining power to publish block before honest nodes

Attacker begins to add blocks to a private copy of the blockchain

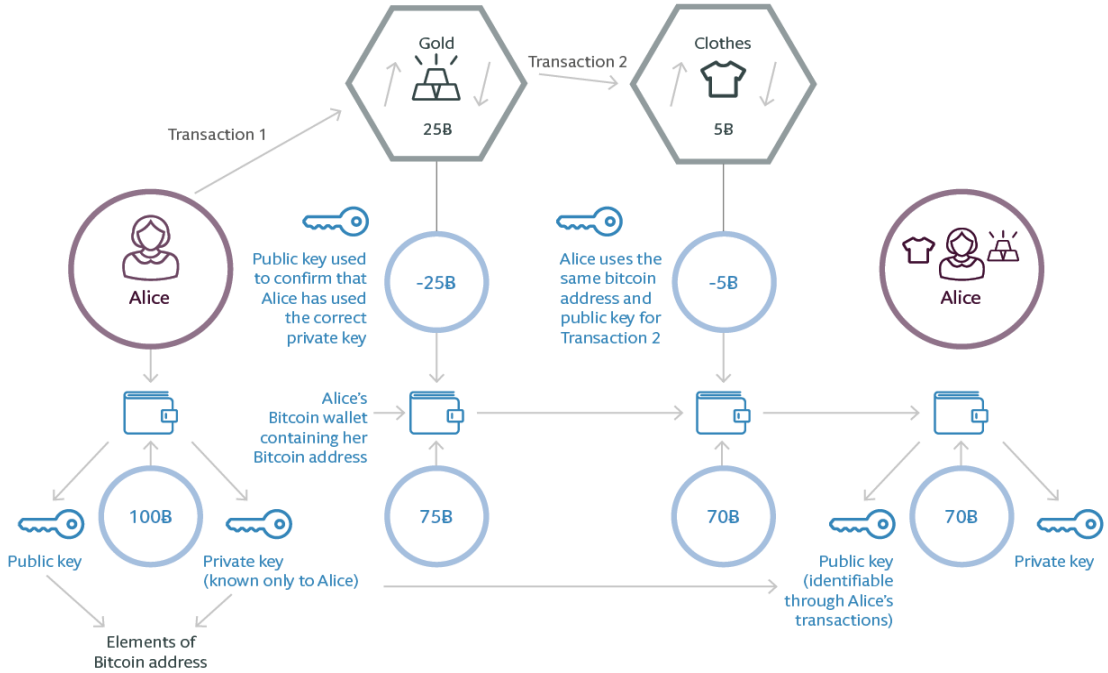
Attacker spends 100 bitcoin on public chain, but does not record this on private chain

Honest nodes follow longest chain – attacker retains spent bitcoin

Double spending

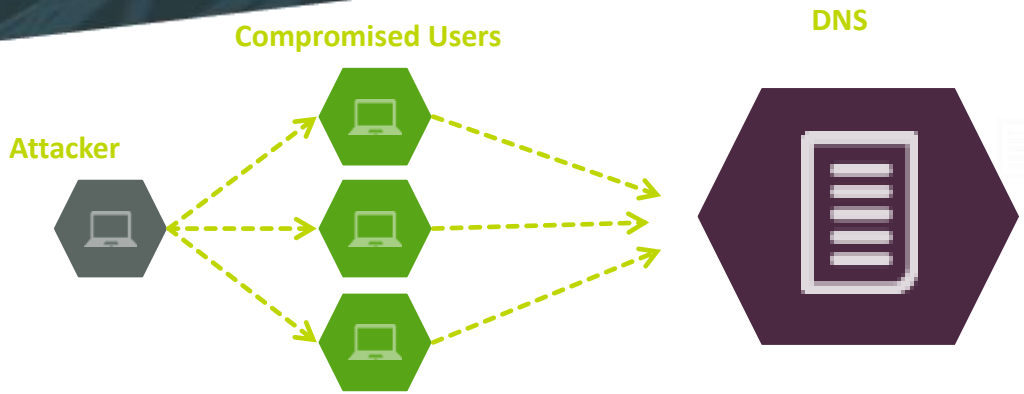
The same currency unit is assigned to multiple users

Multiple users therefore use the same coin simultaneously

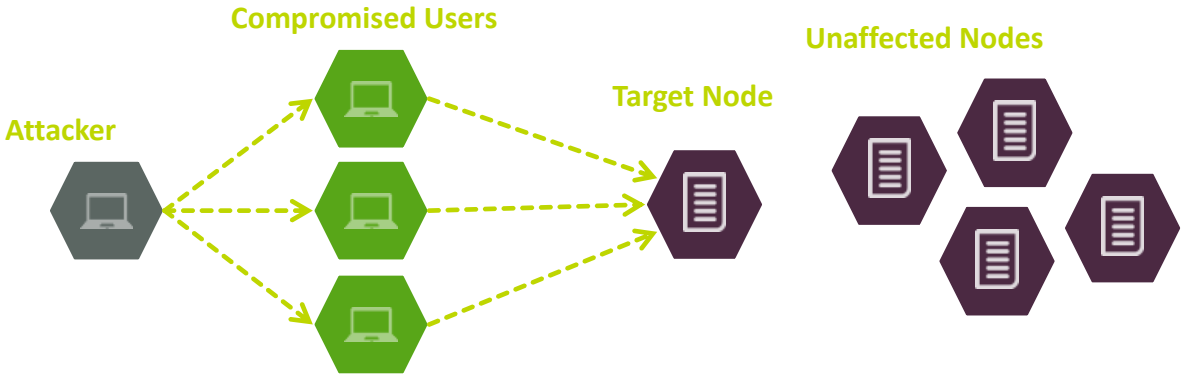


DDoS attacks

Regular DDoS attack

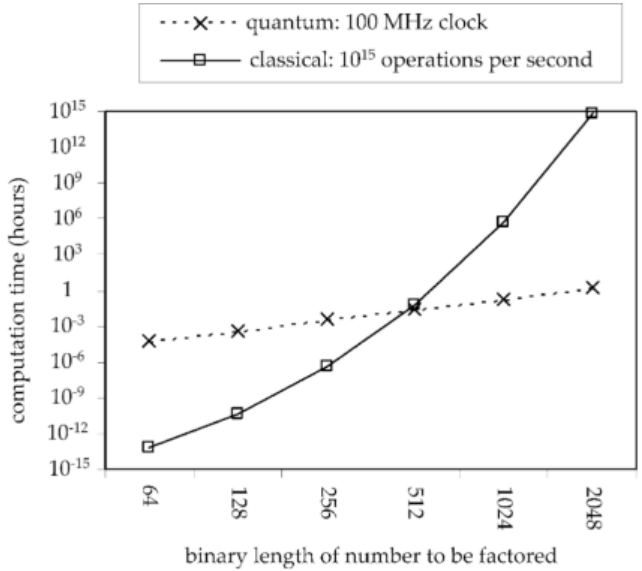


DDoS attack on a blockchain



Quantum computing

- Blockchain is cryptographically secure and has yet to be hacked
- Quantum computing threatens to do this through the vast number of calculations it can process
- Future blockchains may have to incorporate quantum cryptography



GDPR obligations

Legislation

General Data Protection Regulation 2016

Who does it apply to?

Controllers and processors

Security obligations

Pseudonymisation and encryption of personal data
Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems
Ability to restore availability and access to personal data in the event of a physical or technical incident
Process for regularly testing, assessing and evaluating effectiveness of technical and organisational security measures

Breach notification

Notify to supervisory authority within 72 hours of becoming aware of breach
Notify affected data subjects

NIS obligations

Legislation

Network and Information Security Directive 2016

Who does it apply to?

Operators of essential services (infrastructure)
Online marketplaces
Online search engines
Cloud computing service providers

Security obligations

Member States require to have a national framework to manage cyber security incidents
Cooperation group required among Member States to support and facilitate strategic cooperation and exchange of information
Must take appropriate and proportionate security measures to manage risks to networks and information systems

Breach notification

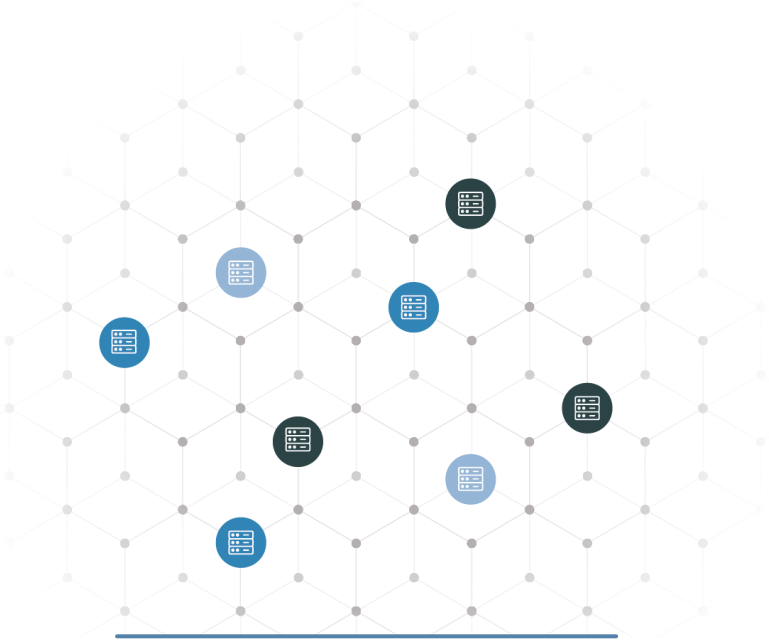
Notify the relevant national authority

Smart contracts

Is it a contract

Jurisdiction and governing law

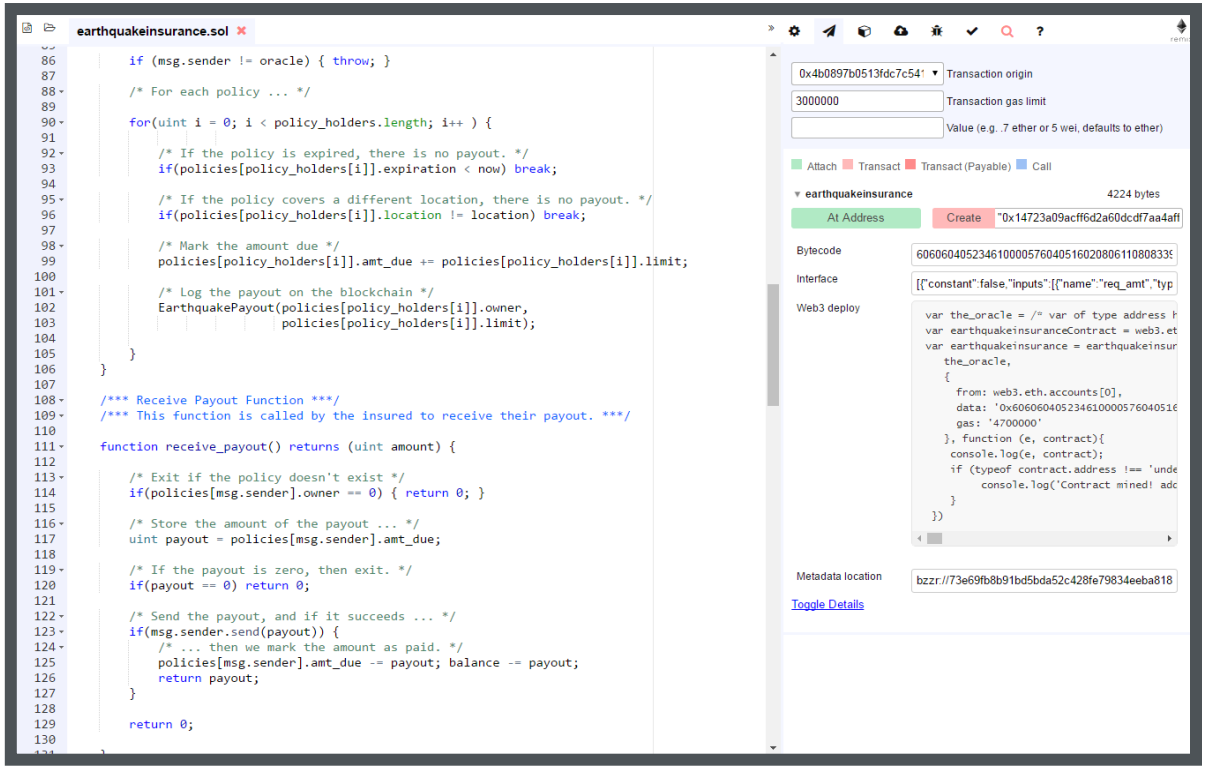
Interpretation of underlying intention



Decentralised company
(blockchain)

What is a smart contract?

- Neither smart nor a contract
- Computer programme designed to implement an agreement



What is a smart contract?

- A programmable computer protocol that can automatically execute the terms of a contract
- Despite not being a contract itself, contract law can apply

Why use a smart contract?

- Automatic execution reduces contracting risks
  - deliberate non-performance
  - third-party interference
  - force majeure
- Less ambiguity – computer programmes require precision
- Standardisation – reliably repeatable performance
- Fraud avoidance – contract stored “permanently”

Key legal challenges
Contract law

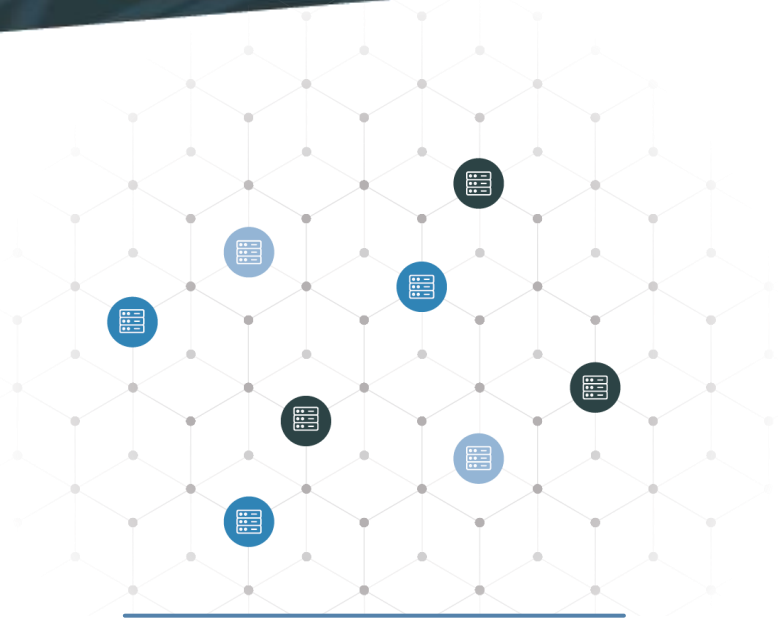
- Which law applies?
- Is a smart contract the contract or just a part of the contract?
- Is the smart contract enforceable?
  - What elements are required to make computer code an enforceable contract?
  - What happens if there is a conflict between the parties' intentions and the smart contract code?

Key legal challenges
Contract law

- **Unlikely that a smart contract is the whole agreement**
  - Usually only a few clauses of an agreement require action by the parties
  - Typical agreement boilerplate cannot be coded as a smart contract
- **Written agreement v smart contract:**
  - Is the contract the written agreement alone?
  - Is the contract the smart contract alone?
  - Is the contract the written agreement plus the smart contract?
- **Smart contracts need to be carefully designed**
  - Comply with all applicable laws and regulations
  - Implement parties' intentions and be fully enforceable

Deposit Guarantee Scheme Directive (DGSD)

The DGSD aims to harmonise depositor protection within the EU, including a definition of what constitutes a bank deposit



The prospectus rules should apply to cryptoassets offered to the public, including through an ICO, where the instruments qualify as transferable securities

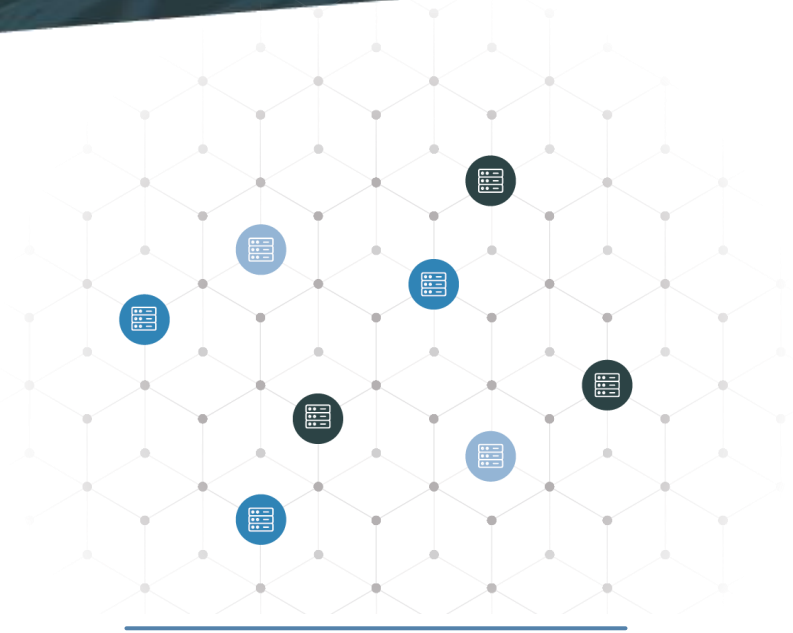
Prospectus Directive

The Prospectus Directive requires publication of a prospectus before the offer of securities to the public or the admission to trading of such securities on a regulated market situated or operating within a Member State

The prospectus rules should apply to cryptoassets offered to the public, including through an ICO, where the instruments qualify as transferable securities

Transparency Directive

The Transparency Directive aims to provide the disclosure of accurate, comprehensive and timely information about issuers whose securities are admitted to trading on a regulated market situated or operating within a Member State



Where the cryptoassets are transferable securities admitted to trading on a regulated market situated or operating within a Member State, their issuers will therefore need to comply with the periodic and ongoing disclosure requirements set in the Transparency Directive

Markets in Financial Instruments Directive

A firm that provides investment services/activities in relation to financial instruments as defined by MiFID II needs to be authorised as an investment firm and comply with MiFID II requirements

Cryptoassets that are deemed to be transferable securities will have to comply with this Directive

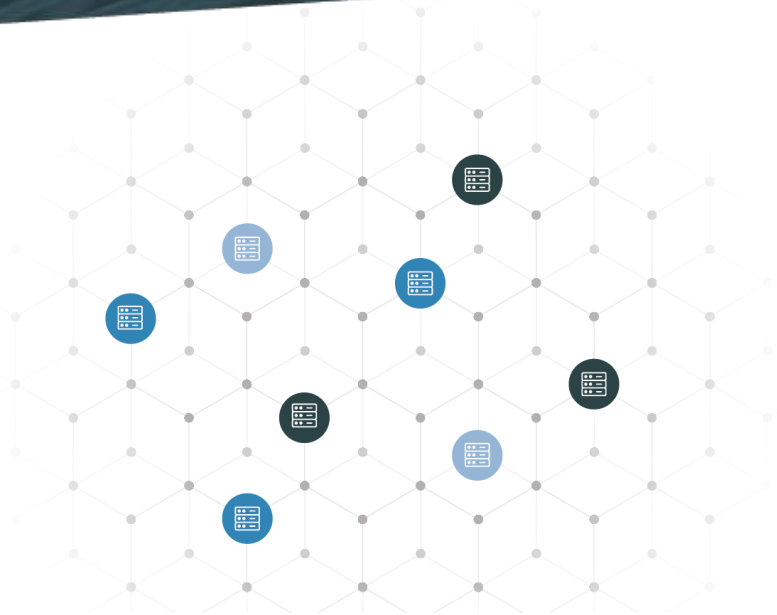
Market Abuse Regulation

The MAR prohibits insider dealing, the unlawful disclosure of inside information and market manipulation (market abuse)

The novel nature of cryptoasset market could mean that some new abusive behaviours may arise which are not directly captured by MAR or current market monitoring arrangements

The Settlement Finality Directive and Central Securities Depositories Regulation

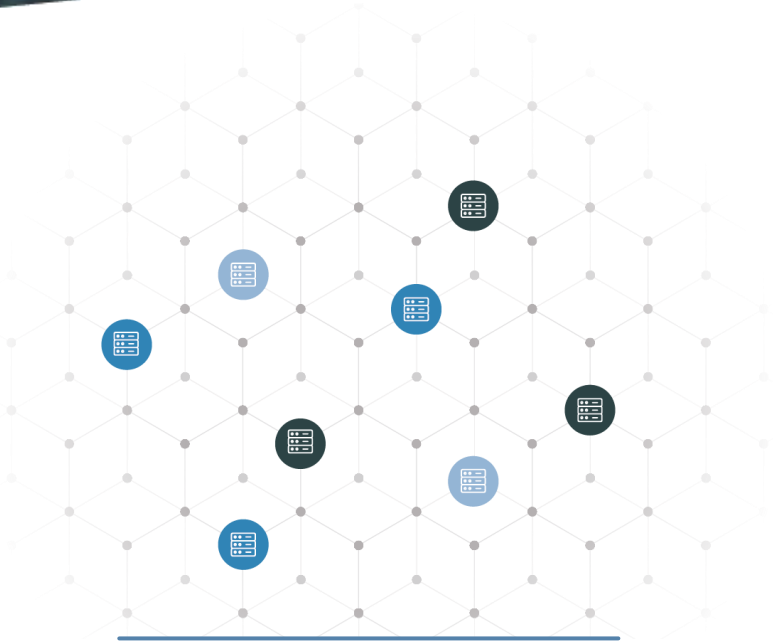
The aim of the Central Securities Depositories Regulation (CSDR) is to harmonise certain aspects of the settlement cycle, settlement discipline and provide a set of common requirements for CSDs operating securities settlement systems in order to enhance cross border settlement in the EU



Where cryptoassets qualify as transferable securities and are traded on trading venues, their issuer, provided it is established in the EU, shall arrange for such securities to be represented in book-entry form with an authorised CSD

AIFMD

The Alternative Investment Fund Managers Directive (AIFMD) lays down requirements for the authorisation, organisation, business conduct and transparency of managers of alternative investment funds



Some cryptoassets may qualify as units in collective investment undertakings, most likely AIFs. Further analysis will be required to assess whether those cases may fall within the scope of the AIFMD

Directive on Investor Compensation Schemes

The Directive on Investor Compensation Schemes provides access to compensation up to a specified amount for investors where the investment firm is no longer financially able to meet its obligations and requires all authorised investment firms to belong to such a scheme

Applicable to crypto firms in so far as they fall within the remit of being a MiFID firm

Hogan Lovells

www.hoganlovells.com