Asia-Pacific
Economic Cooperation

2018/SOM1/EC/WKSP2/005a

Blockchain and Smart Contract for Contract Management (Dispute Prevention and Generation) - Presentation

Submitted by: Doshisha University

APEC 2018
PAPUA NEW
GUINEA

Workshop on the Use of Modern Technology for Dispute Resolution and Electronic Agreement Management Particularly Online Dispute Resolution
Port Moresby, Papua New Guinea
3-4 March 2018

Blockchain and Smart Contract for Contract Management (Dispute Prevention and Generation)

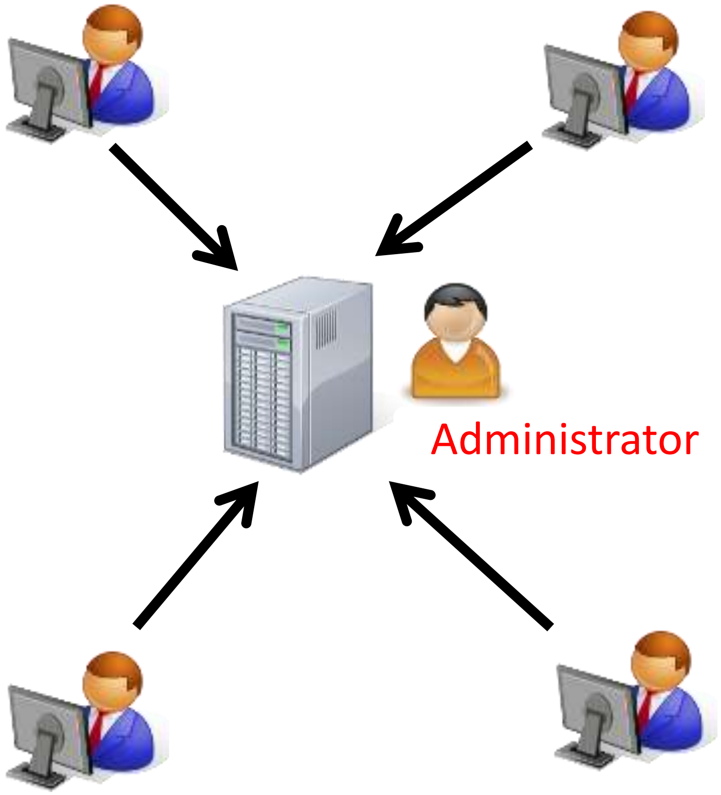
APEC Workshop on the Use of Modern Technology for Dispute Resolution and Electronic Agreement Management (particularly Online Dispute Resolution)

Port Moresby, 3-4 March 2018

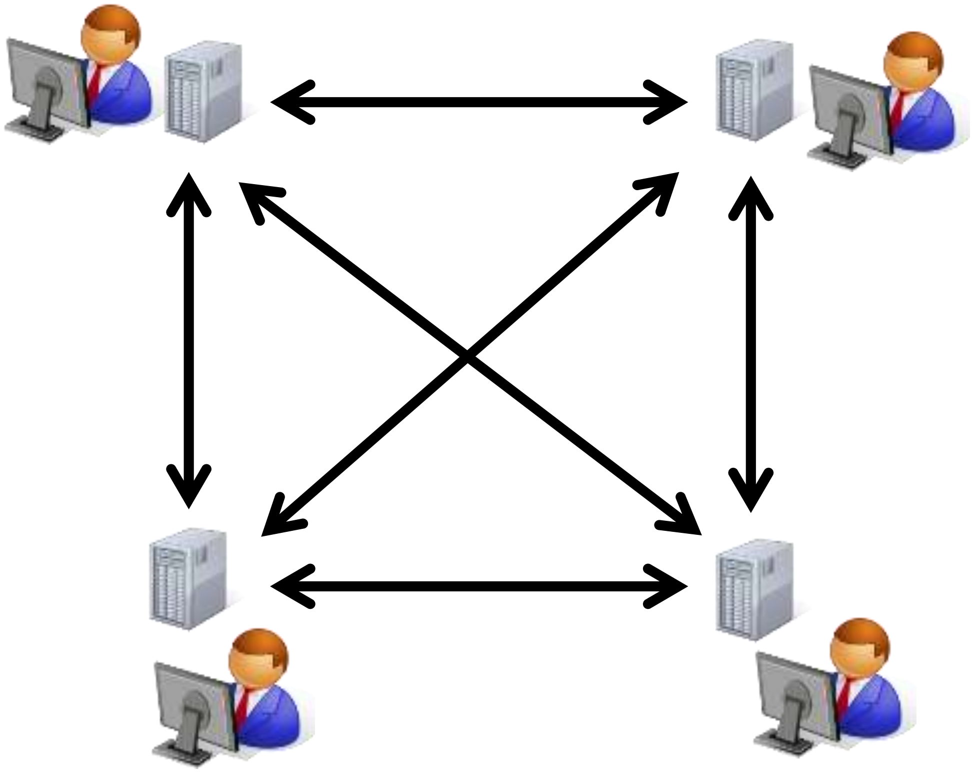
Koji Takahashi (Doshisha University Law School (Japan))

Two Types of Databases

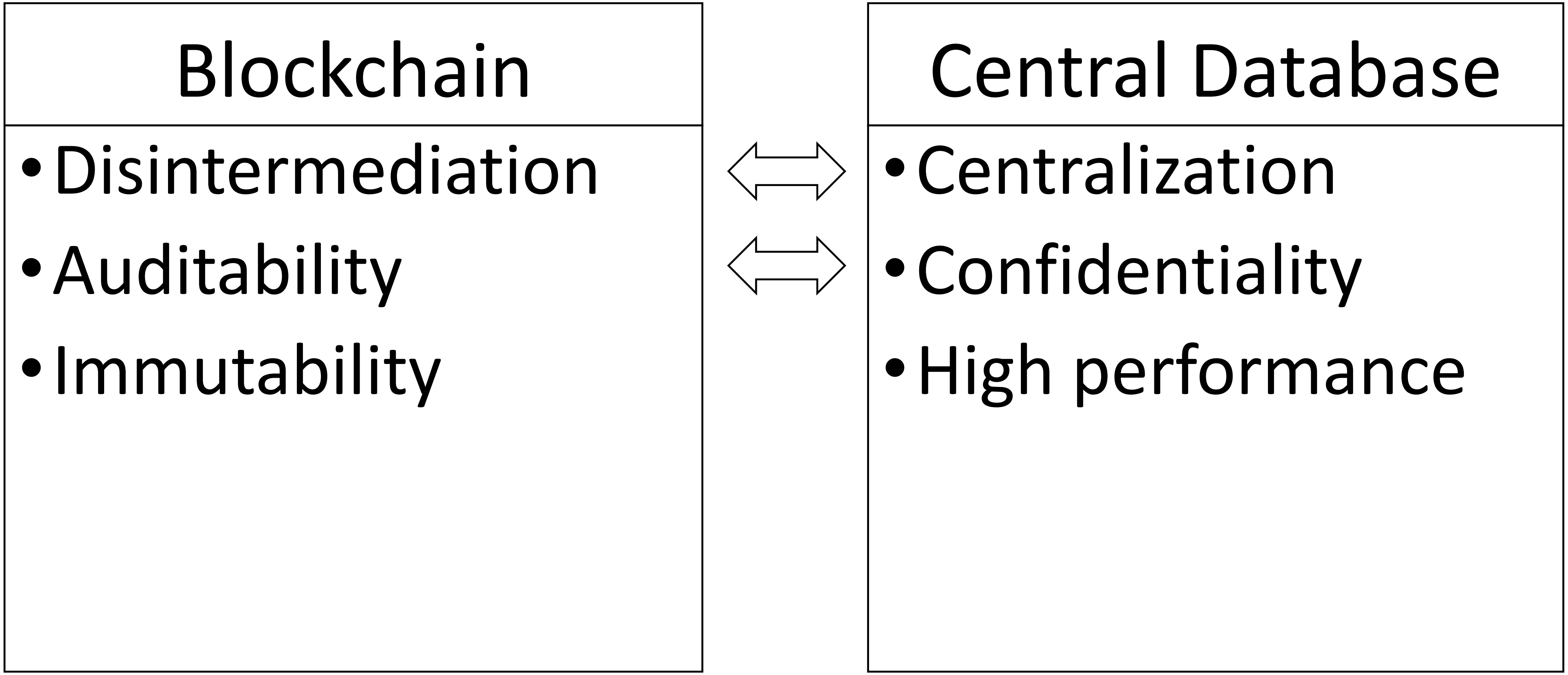
A central database



A blockchain (distributed ledgers)



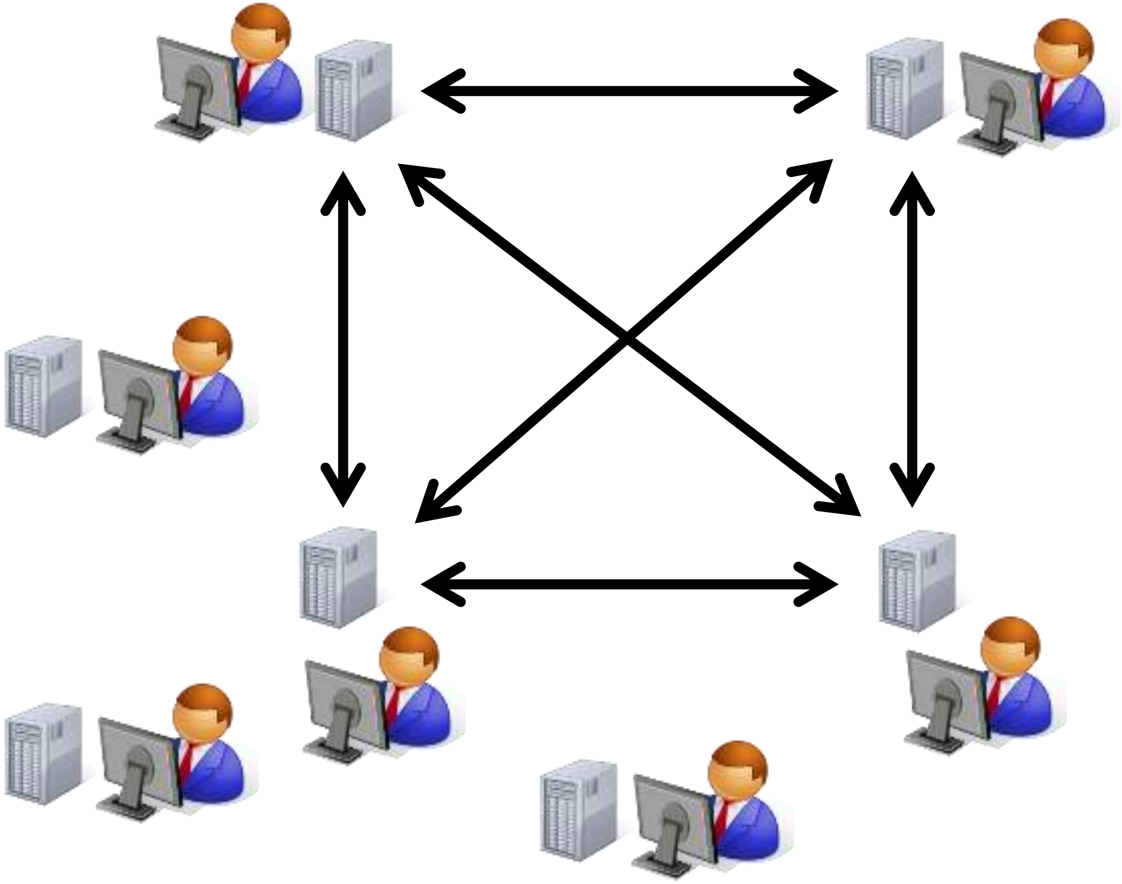
There is no difference with respect to the types of data that can be stored.



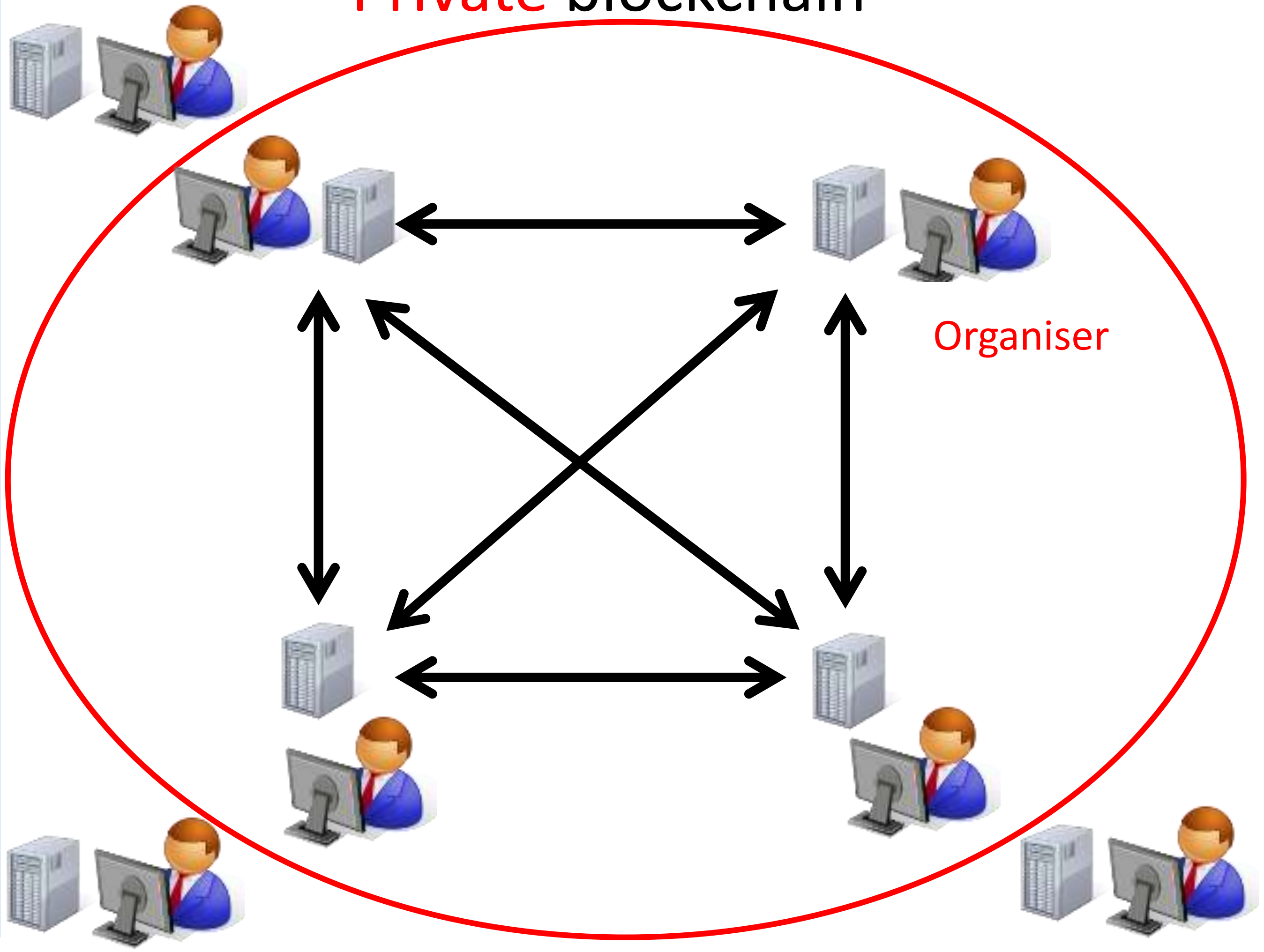
Blockchain		Central Database
• Disintermediation	⟺	• Centralization
• Auditability	⟺	• Confidentiality
• Immutability		• High performance

Two Types of Blockchains

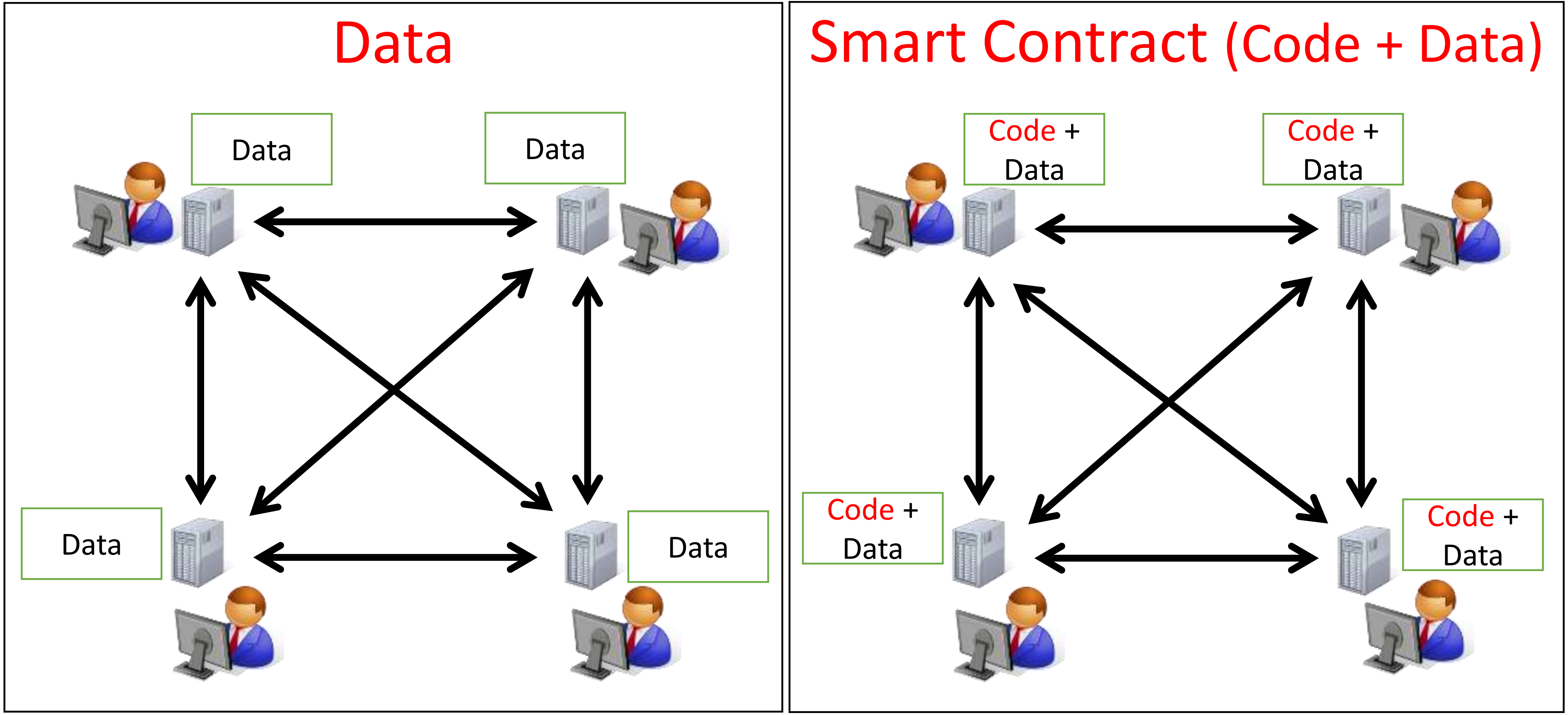
Public blockchain



Private blockchain



Blockchain



Data

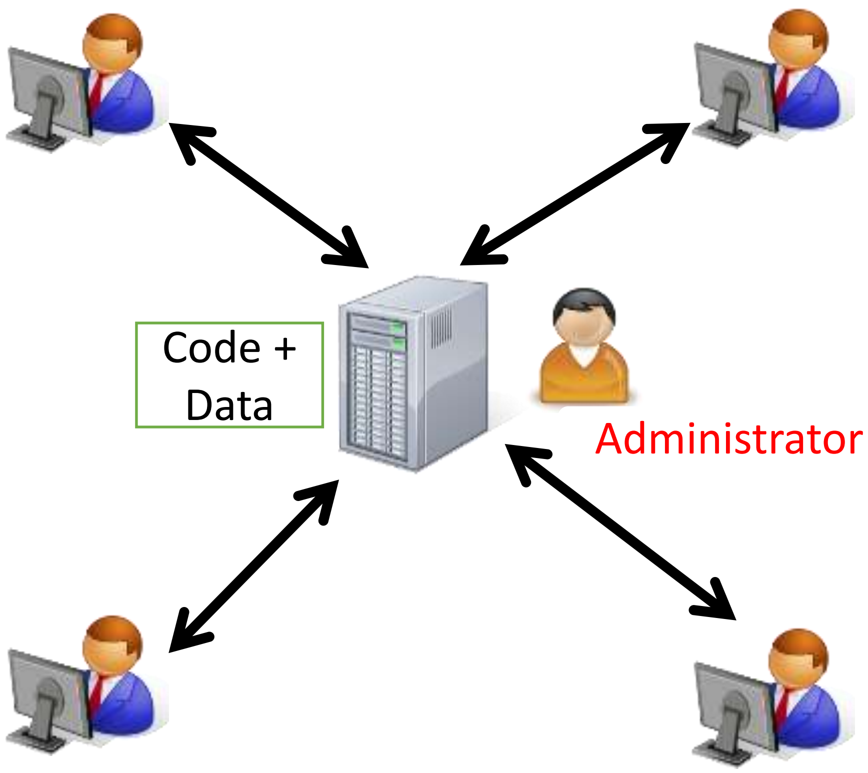
Smart Contract (Code + Data)

Smart Contract

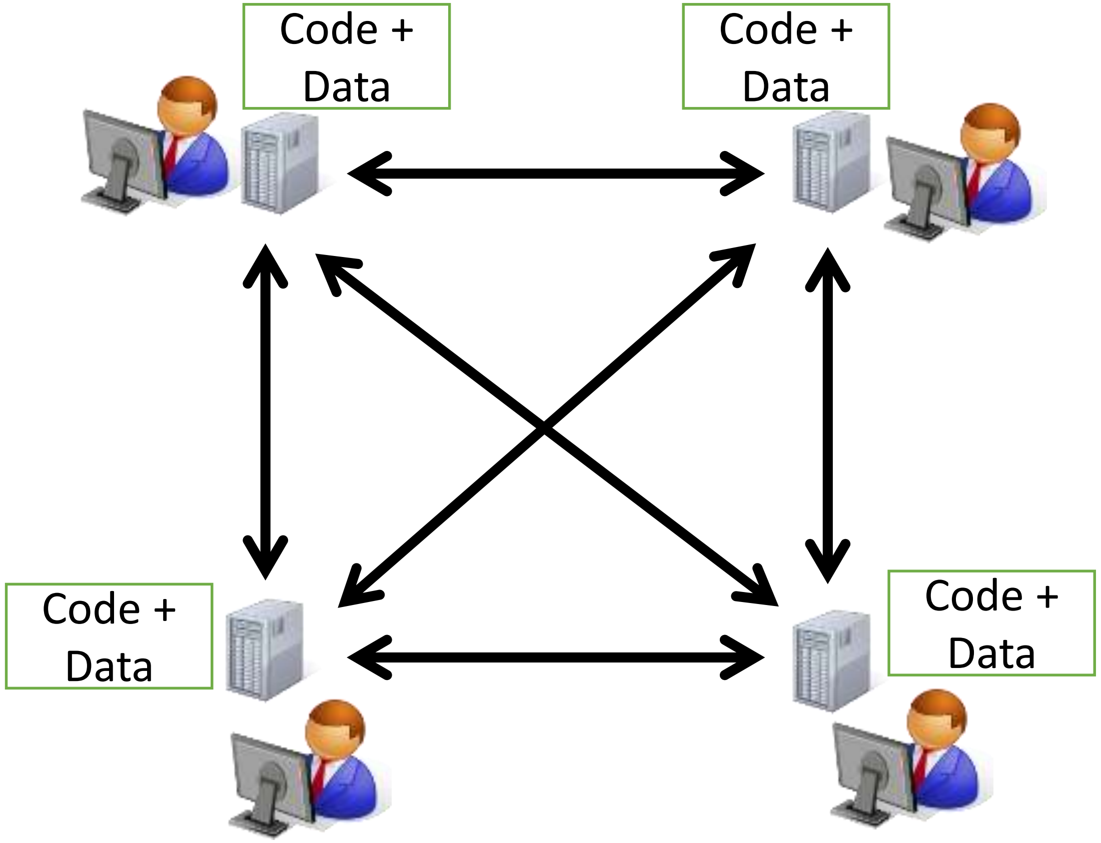
- A computer code with an associated database which runs on every node in a blockchain.
- DAO (Decentralized Autonomous Organization) = Smart contracts structured to emulate an organization with a decision-making apparatus.

Central Server vs Blockchain

A central Server



Blockchain (Smart Contract)



Smart Contract on Blockchain		**Code on Central Server**
• Disintermediation	⇔	• Centralization
• Auditability	⇔	• Confidentiality
• Immutability		• High performance
• Flexibility only if “Turing complete”	⇔	• Flexibility

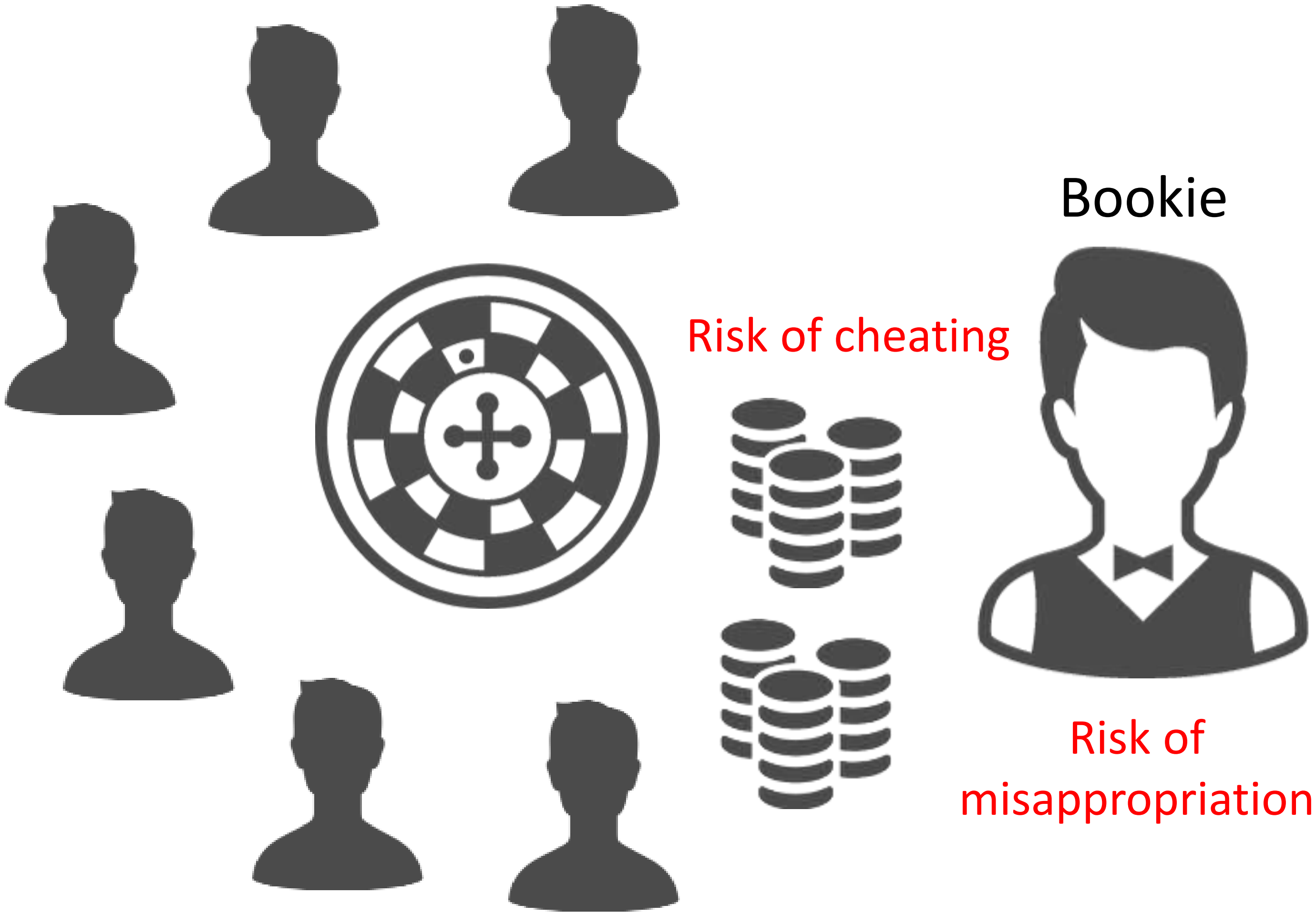
Contract Management

- Smart contract = a computer code ≠ legal contract.
- A smart contract can be a tool for performing a legal contract.
  - But a smart contract can only interact with data on a blockchain.
- A legal contract may incorporate a smart contract by reference.
  - Not wise but freedom of contract.
  - Limitations
    - Limitation to foresight
    - Unfit for general notions, e.g. good faith, force majeure

Smart Contract
Dispute Prevention

- In common with a computer code on a central server
  - To the extent programmable, ambiguity can be avoided.
  - To the extent performance is automated, default can be avoided.
- Uniquely to a smart contract
  - Disintermediation, auditability and immutability
    - → No room for cheating by intermediaries
    - → No single point of failure or attack

Betting in Casino (Prediction Market)



Bookie

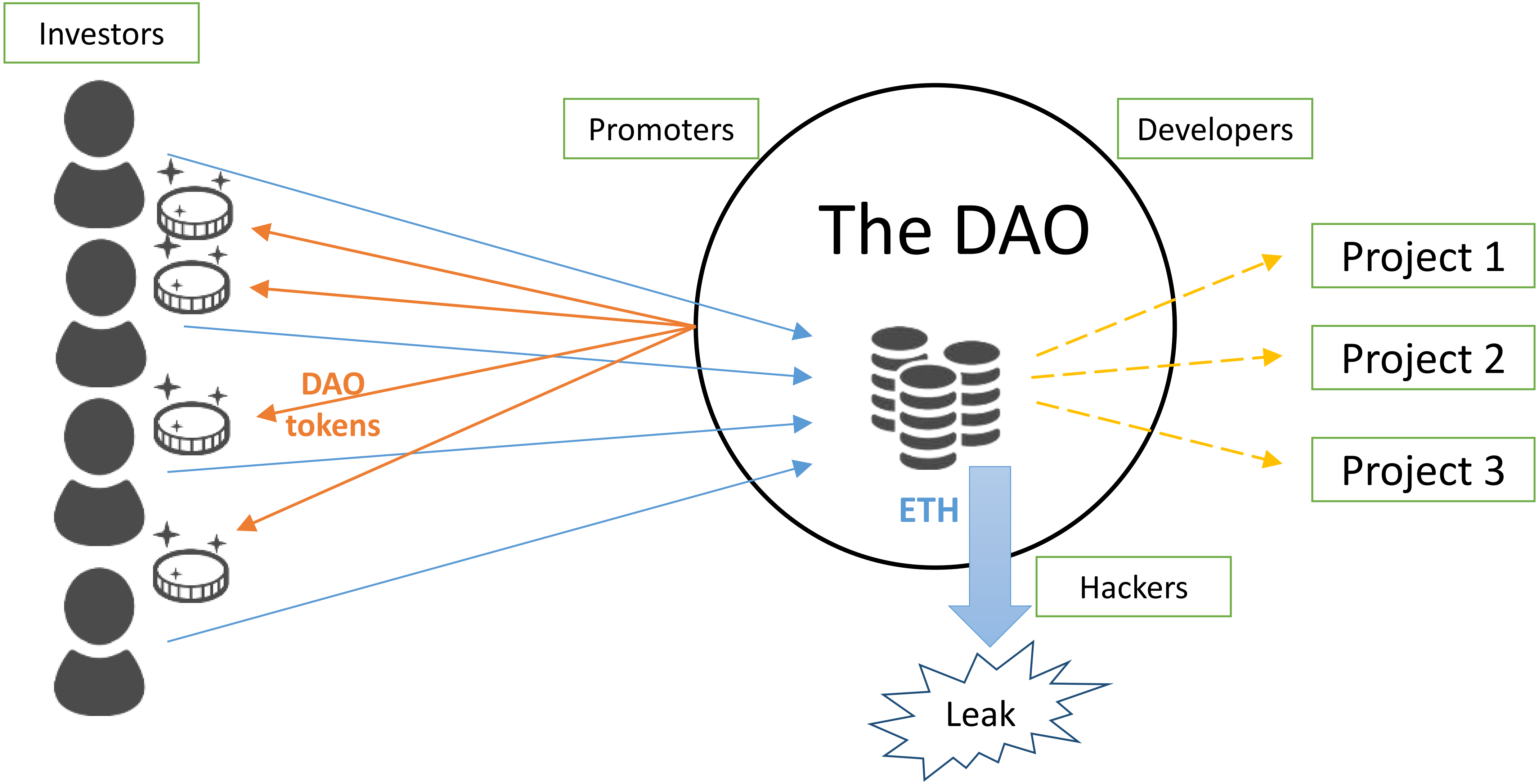
Risk of cheating

Risk of misappropriation

Smart Contract Dispute Generation

- Auditability and immutability can be a fertile ground for disputes.
  - A smart contract has produced results at odds with the underlying legal contract.
  - A smart contract has been executed notwithstanding that the underlying legal contract has been annulled or terminated.
  - A bug in a smart contract has been exploited by hackers.
- Some novel legal issues.

The DAO Failure (2016)



Whether a DAO can sue or be sued

- Once a DAO is deployed, no person has control over it.
- But it has no legal personality.
- The U.S. Securities and Exchange Commission: “The DAO, an unincorporated organization, was an issuer of securities.”
  - “issuer” = “every person who issues … any security.”
  - “person” includes “any unincorporated organization.” 15 U.S.C. § 77b(a)(4).
- What if in a private law context?

Liability of Developers and Promoters

- Hackers, due to pseudonymity, may not be identified.
- There is no administrator of a DAO.
- Developers of the code?
  - No computer code is immune from errors.
  - What if they are anonymous?
- Promotors of the DAO?
  - A team of volunteers promoted The DAO at https://daohub.org.
  - What if they acted *pro bono*?
  - What if there are no promoters at all?

Where "Code is Contract"

- Daohub.org: "The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. … The DAO's code controls and sets forth all terms of The DAO Creation."
- The hacker's open letter: "I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether … . … I am making use of this explicitly coded feature as per the smart contract terms …"

Effect of Entire Agreement Clause

- UNIDROIT Principles of International Commercial Contracts

  Article 2.1.17 (Merger clauses)

  A contract in writing which contains a clause indicating that the writing completely embodies the terms on which the parties have agreed cannot be contradicted or supplemented by evidence of prior statements or agreements. However, such statements or agreements may be used to interpret the writing.

  Article 1.4 (Mandatory rules)

  Nothing in these Principles shall restrict the application of mandatory rules, whether of national, international or supranational origin, which are applicable in accordance with the relevant rules of private international law.

Interpretation of Contract

- Article 4.1 (Intention of the parties)

  (1) A contract shall be interpreted according to the common intention of the parties.

  (2) If such an intention cannot be established, the contract shall be interpreted according to the meaning that reasonable persons of the same kind as the parties would give to it in the same circumstances.

- Article 4.3 (Relevant circumstances)

  In applying Articles 4.1 …, regard shall be had to all the circumstances, including

  …

  (d) the nature and purpose of the contract;

  (e) the meaning commonly given to terms and expressions in the trade concerned;

  (f) usages.

Whether “Code is Law”

- Law of physics, cf. law of society
- Smart contracts may generate disputes.
- Solutions may only be found in law outside the code.
  - Damages (in tort or contract), restitution (proprietary or in unjust enrichment), specific performance (in tort or contract).
- The same even where “code is contract”.

Dispute Resolution

- Theft of cryptocurrency
  - by hacking exchanges.
    - Mt. Gox (2014) $473 million
    - Bitfinex (2016) $72 million
    - Coincheck (2018) $523 million
    - BitGrail (2018) $170 million
  - by hacking a DAO (Decentralized Autonomous Organization)
    - The DAO (2016)
  - Claims for damages and restitution against the hacker (in tort) and the exchange (or DAO?) (in contract, rei vindicatio, trust)
- Mistaken transfer of cryptocurrency
  - Claim for restitution in unjust enrichment

Litigation or Arbitration

- Expertise in technical matters
- Arbitration needs an agreement to arbitrate
  - Possible in contractual relationships (e.g. contract with an exchange).
  - Unlikely in tort (e.g. a claim against the hackers).
- National courts must have adjudicatory jurisdiction
  - Choice-of-court agreements where possible.
  - Other bases of jurisdiction may require the localization of cryptocurrencies or other tokens – difficult as recorded in ledgers distributed on a borderless blockchain.
    - Proprietary restitution – situs of the object
    - Contractual restitution – place of delivery
    - Tort - place of wrongful act or consequences

Parties

- Capacity of a DAO to be a party to litigation
  - Assimilated to a foundation without legal personality? Who is to represent it?
- Finding out the identity of the defendant (e.g. hacker, recipient of mistaken transfer)
  - Pseudonymity on a blockchain may cause difficulties.

Admissibility and evidential weight of records in a blockchain in Litigation

- in jurisdictions where judges have wide discretion.
- in jurisdictions with strict rules of evidence,

  - e.g. 12 V.S.A. § 1913 (Vermont) (b) Authentication, admissibility, and presumptions.

    (1) A digital record electronically registered in a blockchain shall be self-authenticating … if it is accompanied by a written declaration of a qualified person, made under oath, stating …: …(C) that the record was maintained in the blockchain as a regular conducted activity; and …

    (2) A digital record electronically registered in a blockchain, if accompanied by a declaration that meets the requirements of subdivision (1) of this subsection, shall be considered a record of regularly conducted business activity ….

    (3) The following presumptions apply: (A) A fact or record verified through a valid application of blockchain technology is authentic. …

    (4) A presumption does not extend to the truthfulness … of the contents of the fact or record.

Admissibility and evidential weight of records in a blockchain in Arbitration

- UNCITRAL Model Law on International Commercial Arbitration (2006) Article 19(2)

  The power conferred upon the arbitral tribunal includes the power to determine the admissibility, relevance, materiality and weight of any evidence.

- UNCITRAL Arbitration Rule (as revised in 2010) Article 27(4)

  The arbitral tribunal shall determine the admissibility, relevance, materiality and weight of the evidence offered.

Execution of Decisions (Awards and Judgments)

- Methods depend on the law of the place of execution.
  - Order to transfer cryptocurrency or to disclose private keys.
    - Under the threat of sanctions for contempt of court.
    - May not be effective if the respondent pretends to have forgotten the keys.
  - Seizure of the tangible medium (e.g. hard disc, paper) in which private keys are stored.
- Executory jurisdiction
  - The localization of the cryptocurrency is difficult.
  - Any place where enforcement may be effective?