Blockchain Development
Week: 1
Title: Blockchain

Dr Ian Mitchell

Middlesex University,
Dept. of Computer Science,
London

September 30, 2019

Module Aims

Aims

Blockchain Technology is changing how organisations communicate and operate, with this change there is a challenge and opportunity for Blockchain developers. This module aims to convey the required knowledge underpinning blockchain technology in order to enable students to apply it to develop solutions to practical problems.

Module Objectives

Knowledge

- *Appraise* blockchain types and holistically explain blockchain anatomy
- *Analyse* a domain specific problem and determine applicatbility of a blockchain solution to that problem

Skills

- The design and development of effective blockchain applications

Module Syllabus

CST4025: Syllabus

- Asynchronous and procedural programming pertaining to blockchain applications
- Blockchain data structures for distributed ledger systems
- Access Control Language for distributed ledger systems
- Implementing business logic for a blockchain solution
- Blockchain and complex system development
- Permissioned Blockchain Technologies
- Consensus Engineering
- Blockchain Engineering
- Blockchain Anatomy

Punctuality, Mobiles and Food

Lateness Policy

Please ensure you are on time to sessions as tutors will start sessions promptly. Please note that if you are more than 15 minutes late you will not be permitted to join the session.

Mobile Phones

Please have your phones on silent throughout the session and only use them in an emergency.

Food & Drink

No eating of food in lab or lecture.
Drinks are permitted in sealed containers.

CST4025 – Indicative Lecture Plan.

Week	Title
1	Introduction to Blockchain
2	Composer: Data Modelling
3	Composer: Access Control Language
4	Formative Feedback
5	Asynchronous Programming & Promises
6	Composer: Node.js I
7	Composer: Node.js II
8	Consensus Engineering
9	Smart Contracts
10	Feedback
11	Feedback
12	Presentation

Table: Lecture Plan, these are indicative titles

Administration

Assessment

- 100% coursework
  - CW1: Data Modelling (25%)
  - CW2: Blockchain Development (75%)
- Formative Feedback: Week 4
- Formative Feedback: Week 10 & 11
- Presentation: Week 12
- e-submission for CW1
- hard copy submission for CW2
- comply to template

Structure

- Attendance $> 75\%$
- Resit: 1^{st} August 2020
- Deferral: 1^{st} August 2020
- Office: T108
- Office Hours: Autumn & Winter Terms: Tuesdays 1515-1615hrs; and, Wednesdays 1415-1515hrs
- Teaching:12 * 2 hour Lab; 12 * 1 hour lecture; 9.5 hours independent study
- Mitigating circumstances: see unihelpdesk and apply for deferral

Lecture Aims & Objectives

- Introduction to Blockchain
- Blockchain Anatomy
- centralised vs decentralised
- distributed
- Consensus
- Collaboration
- Security

What?

Blockchain Definition

Append-only immutable distribute ledger forged via consensus on a P2P network

[1]Blockchain is technically just a series of linked blocks but it is commonly use to represent the entire technology. Technically, it should be referred to as Blockchain Technology.

What?

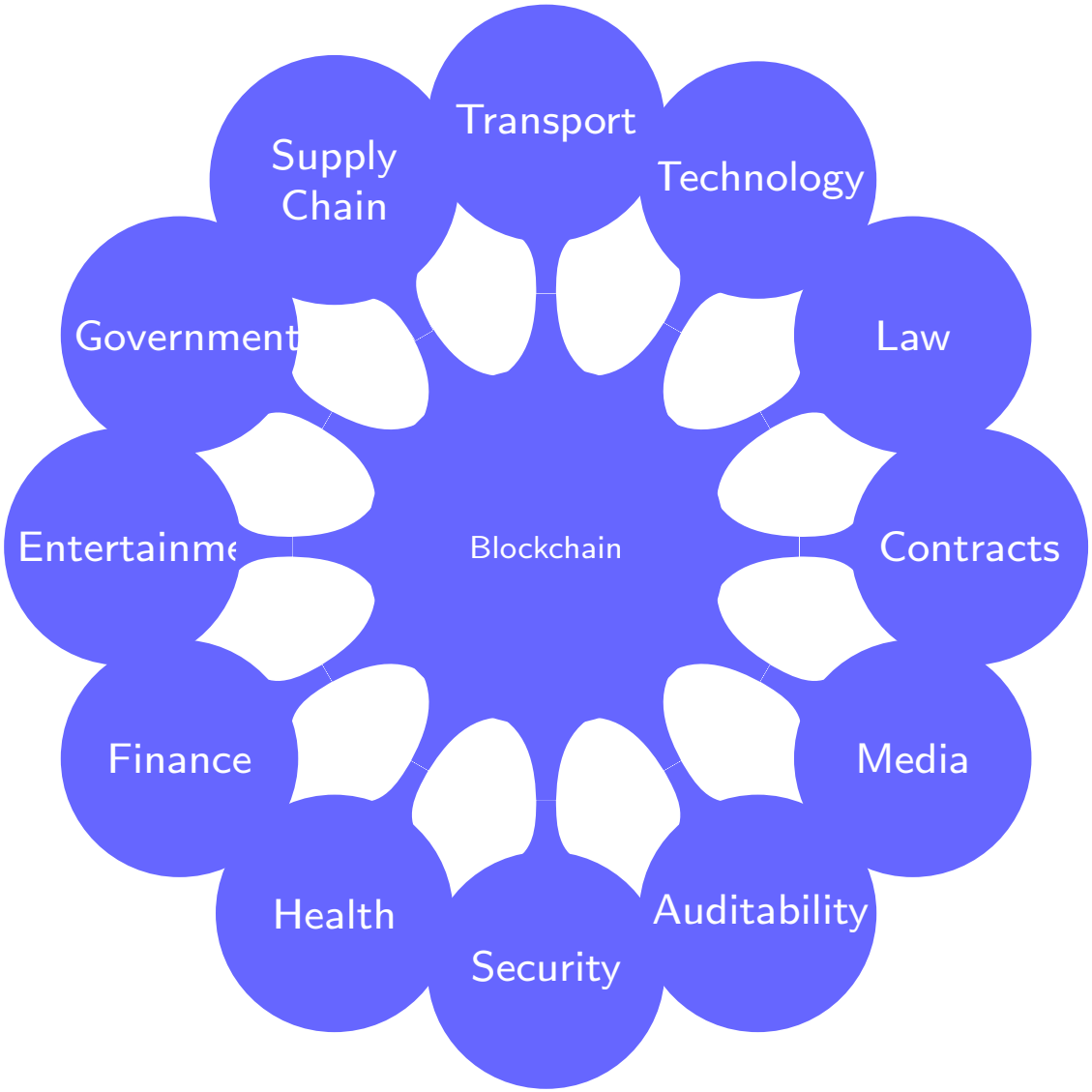
Blockchain Definition

Append-only immutable distribute ledger forged via consensus on a P2P network

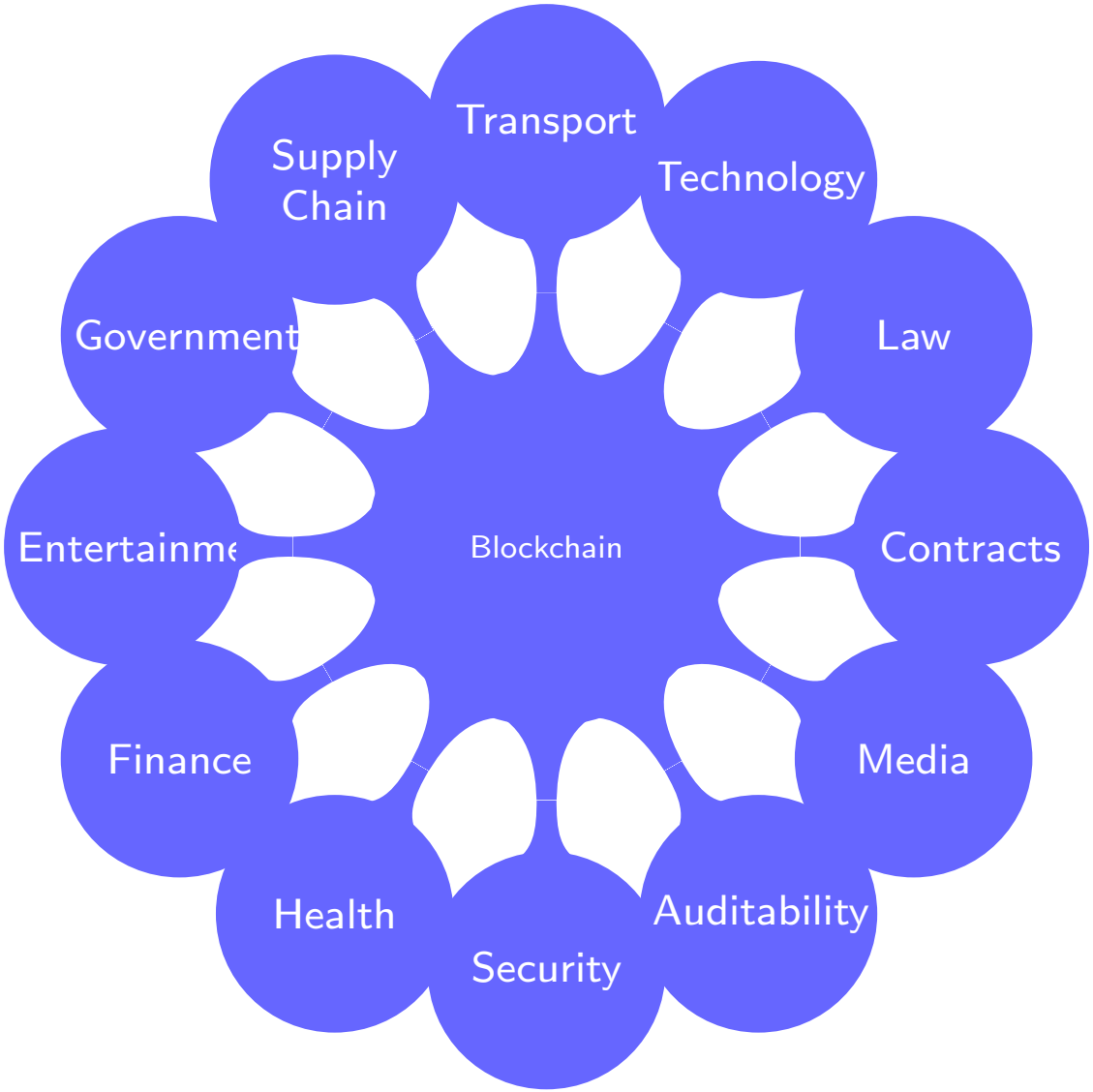
- Decentralised
- Consensus
- P2P
- Blockchain
- Crytography
- Blockchain [1]

[1] Blockchain is technically just a series of linked blocks but it is commonly use to represent the entire technology. Technically, it should be referred to as Blockchain Technology.

Where?

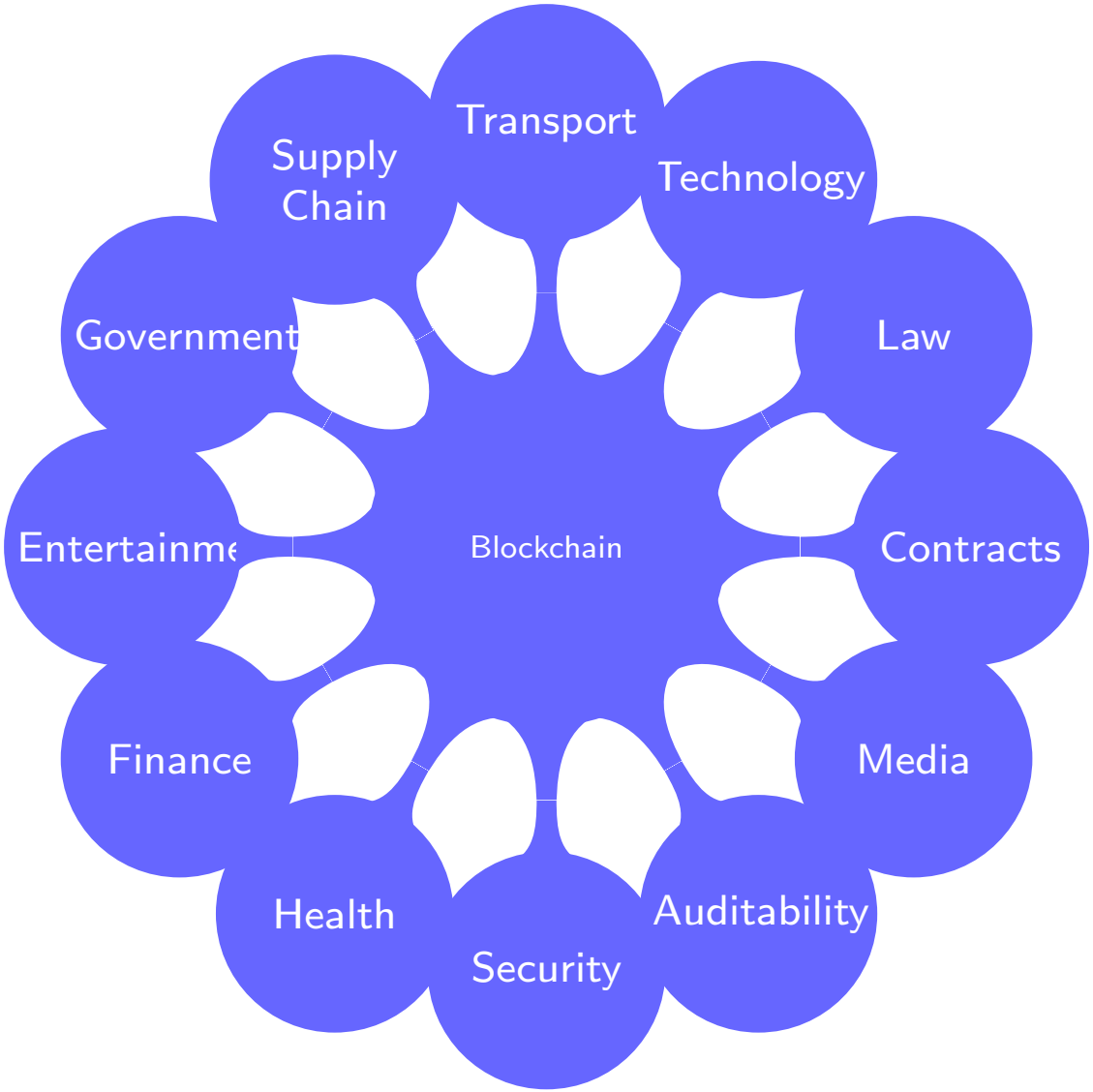

Transport
Technology
Law
Contracts
Media
Auditability
Security
Health
Finance
Entertainme
Government
Supply Chain
Blockchain

Blockchain Mindmap



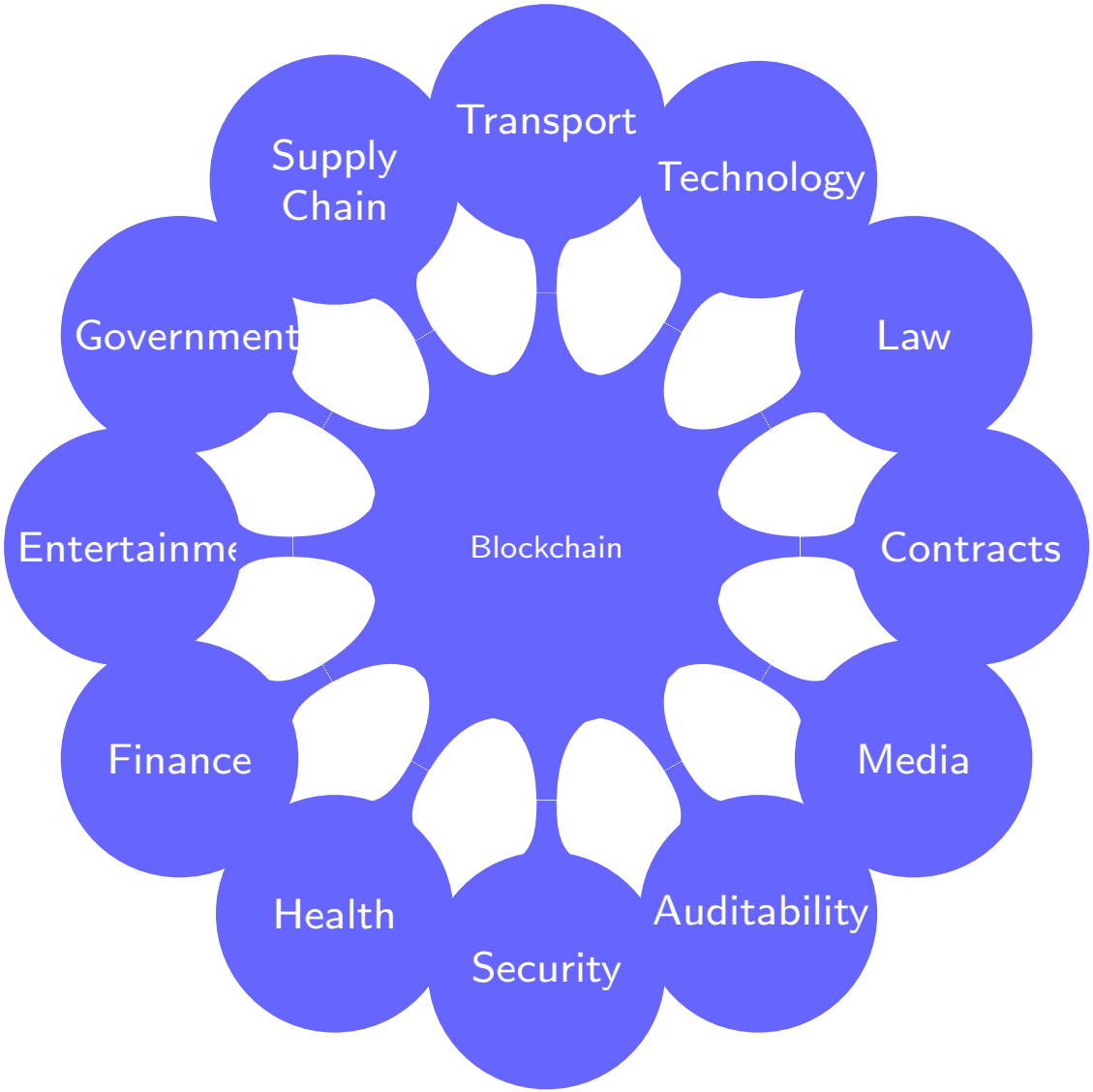
- Contracts
  - Smart Contracts
  - Release payment upon satisfying contractual obligations
  - Ratified by using blockchain

Blockchain Mindmap



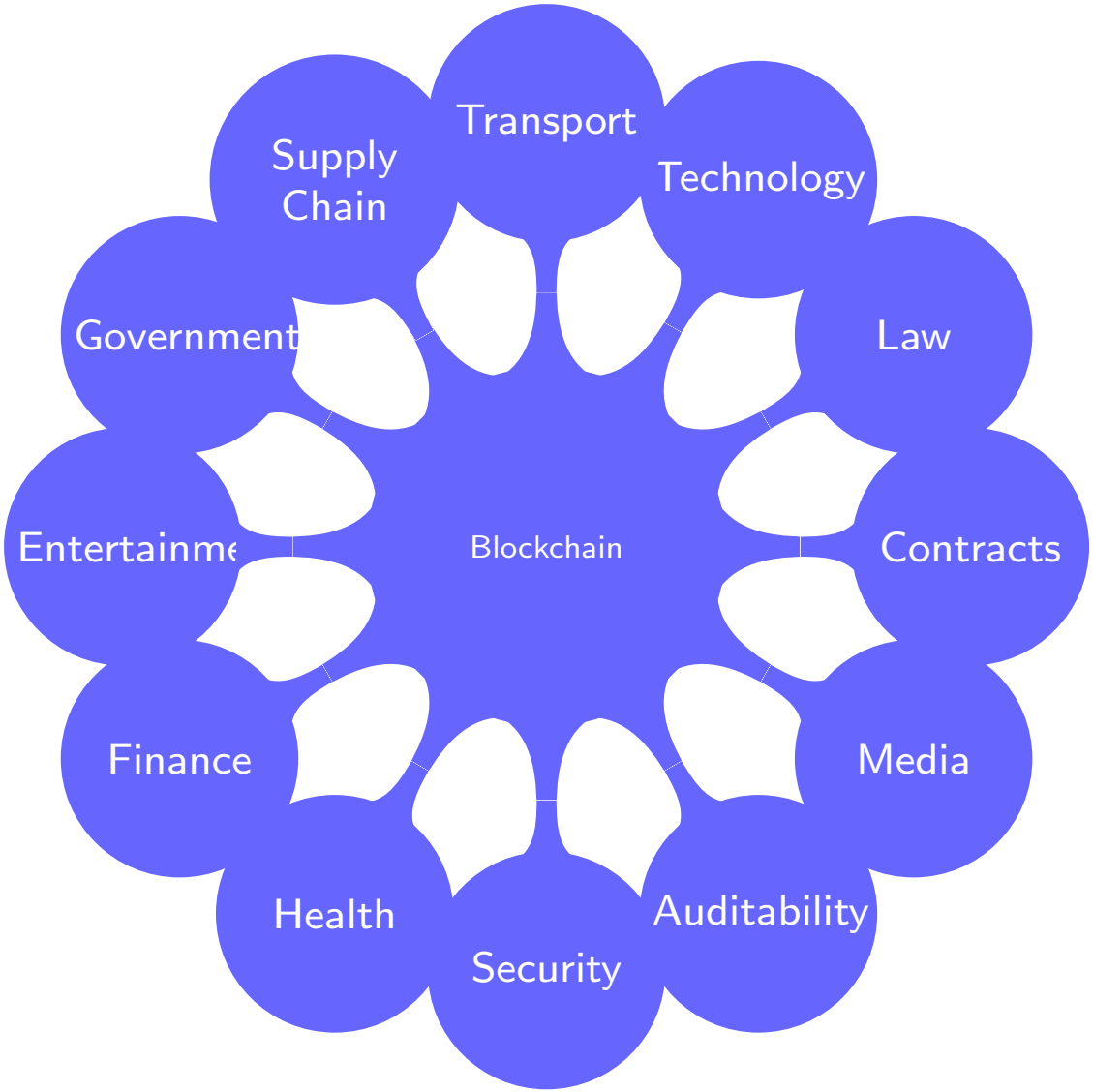
- Law
  - restriction on dangerous items, e.g. gun control
  - Police procedures

Blockchain Mindmap



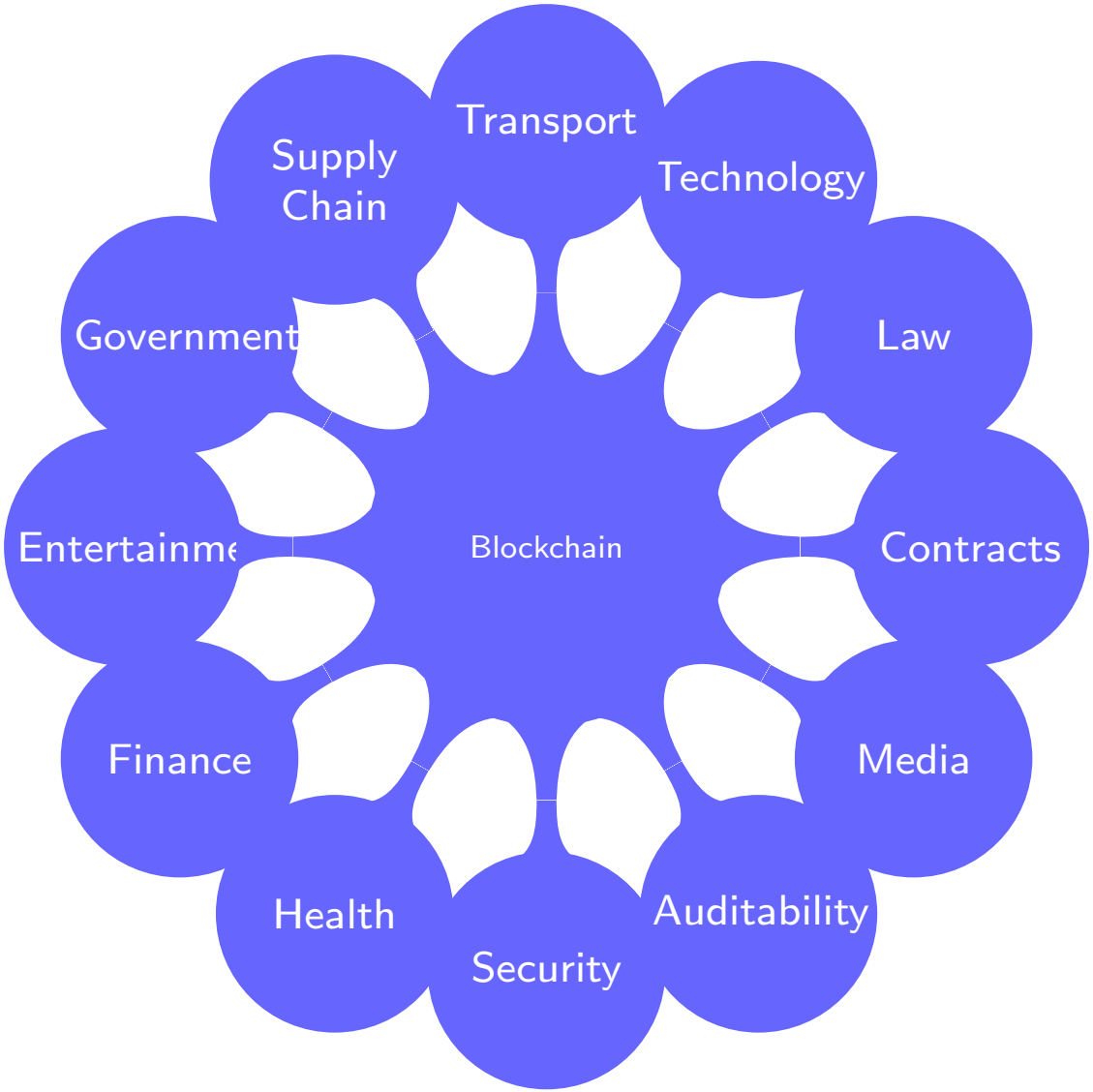
- Technology
  - All areas are seeing blockchain involvement
  - Fridges, Washing machines, smart environments
  - Cyber Security
  - Cloud Storage
  - Internet of Things, IoT

Blockchain Mindmap



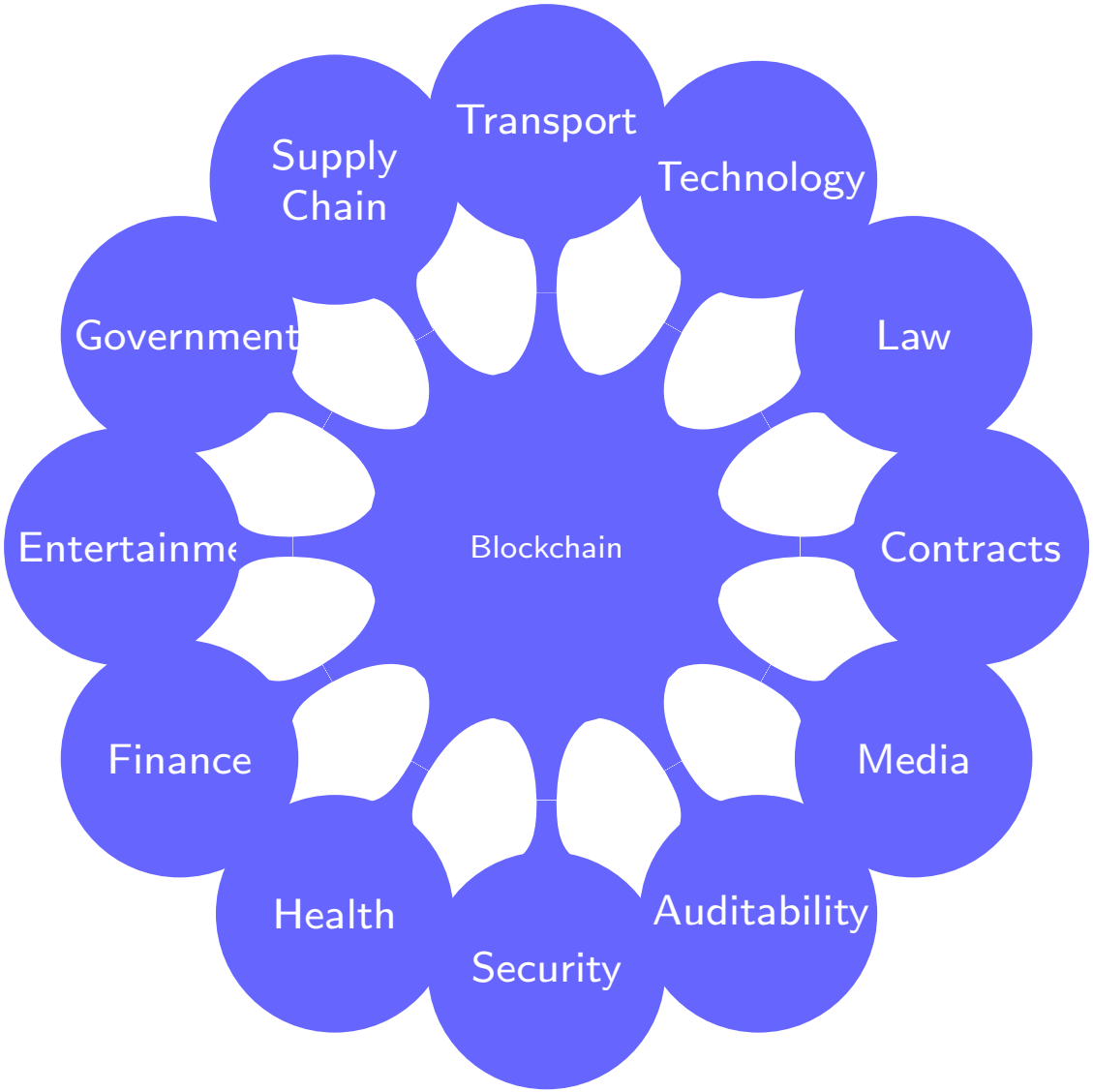
- Transport
  - Public Transportation
  - Automotive
  - Business - fleets of vehicles and navigation

Blockchain Mindmap



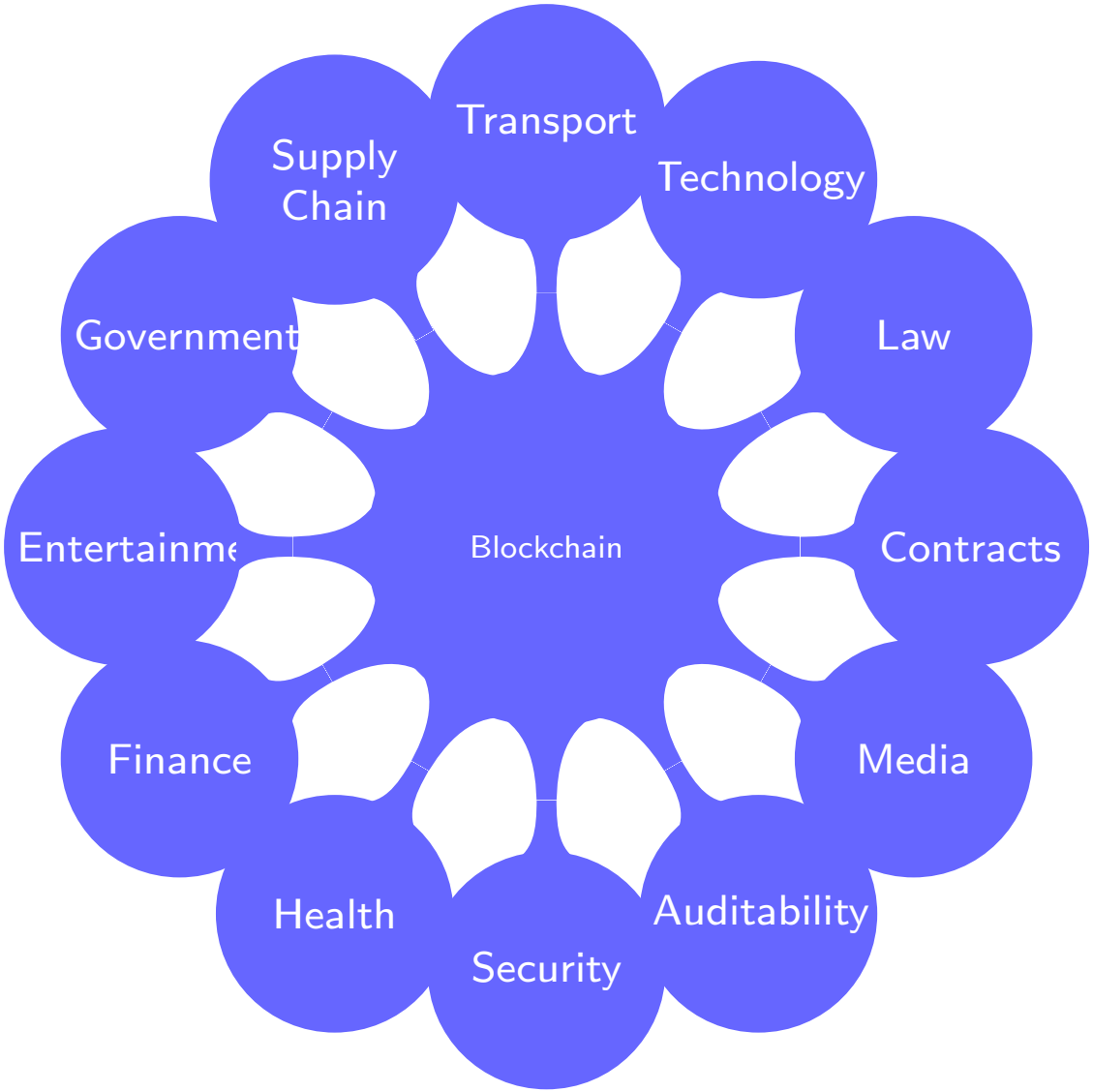
- Supply Chain
  - JIT delivery
  - Pre-conditions
  - Smart contracts
  - Secure
  - Third party
  - Mutual (dis)trust

Blockchain Mindmap



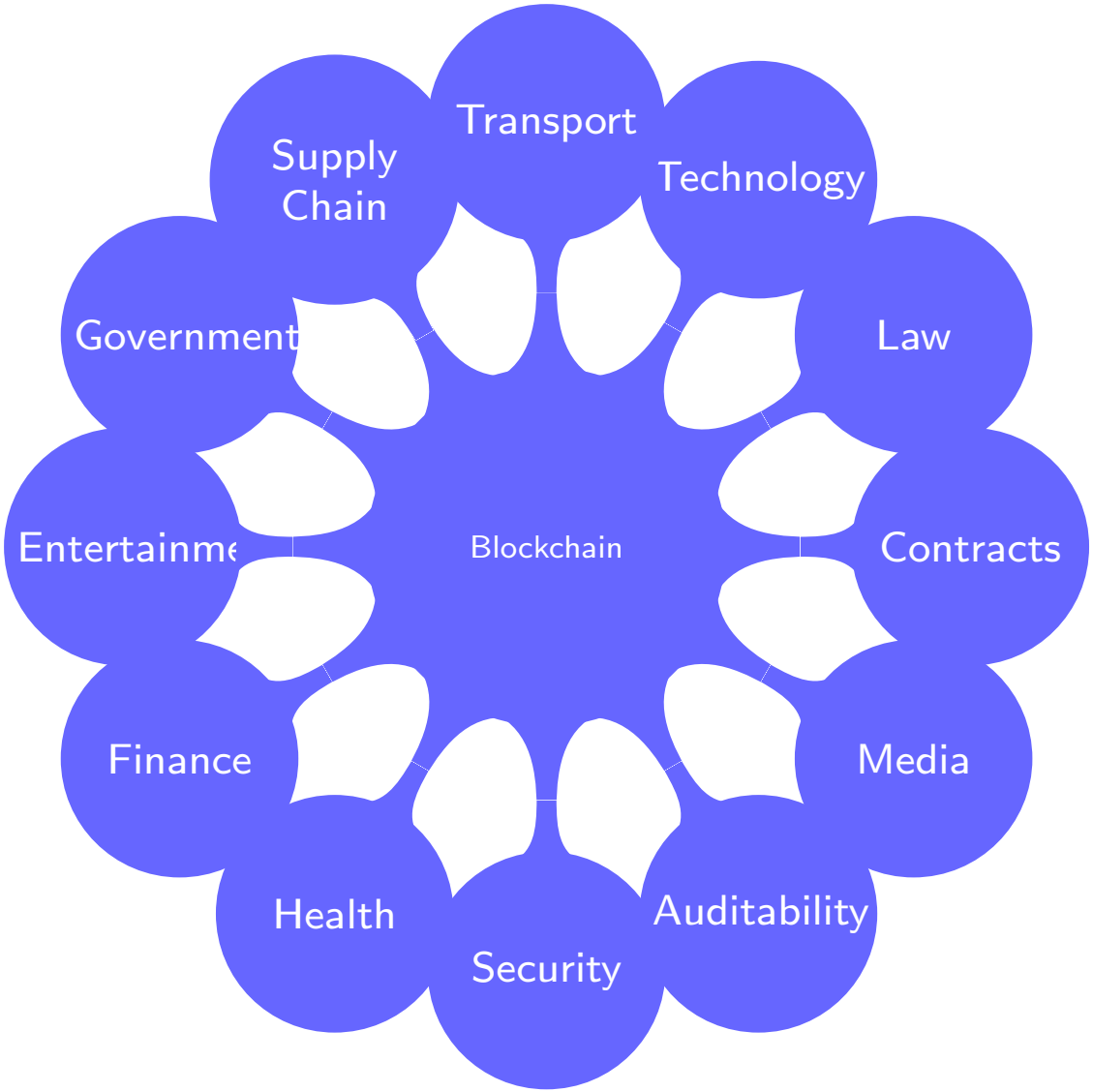
- Government
  - ID Management
  - Electoral
  - Tax

Blockchain Mindmap



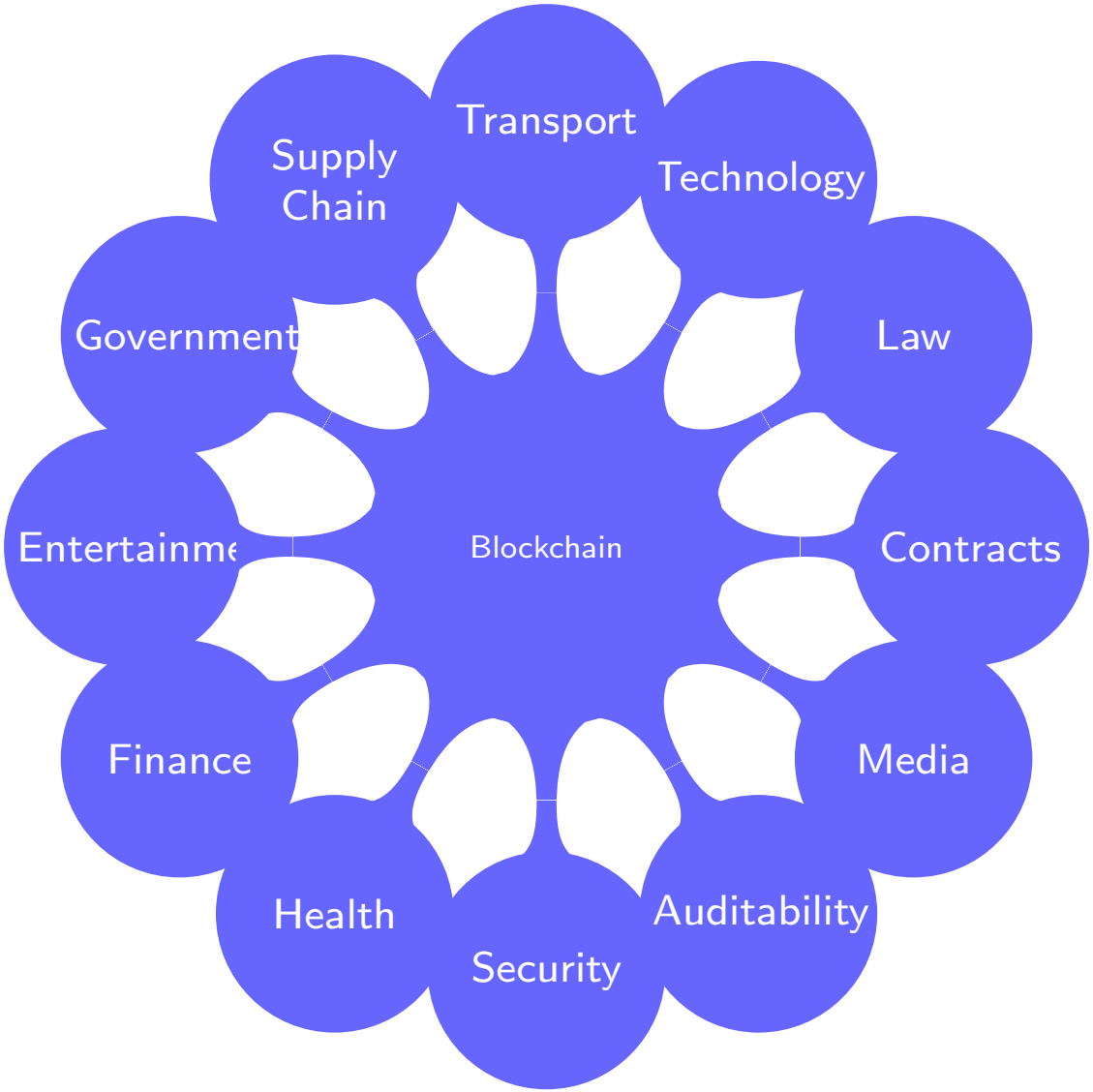
- Entertainment
  - Copyright
  - Digital Rights

Blockchain Mindmap



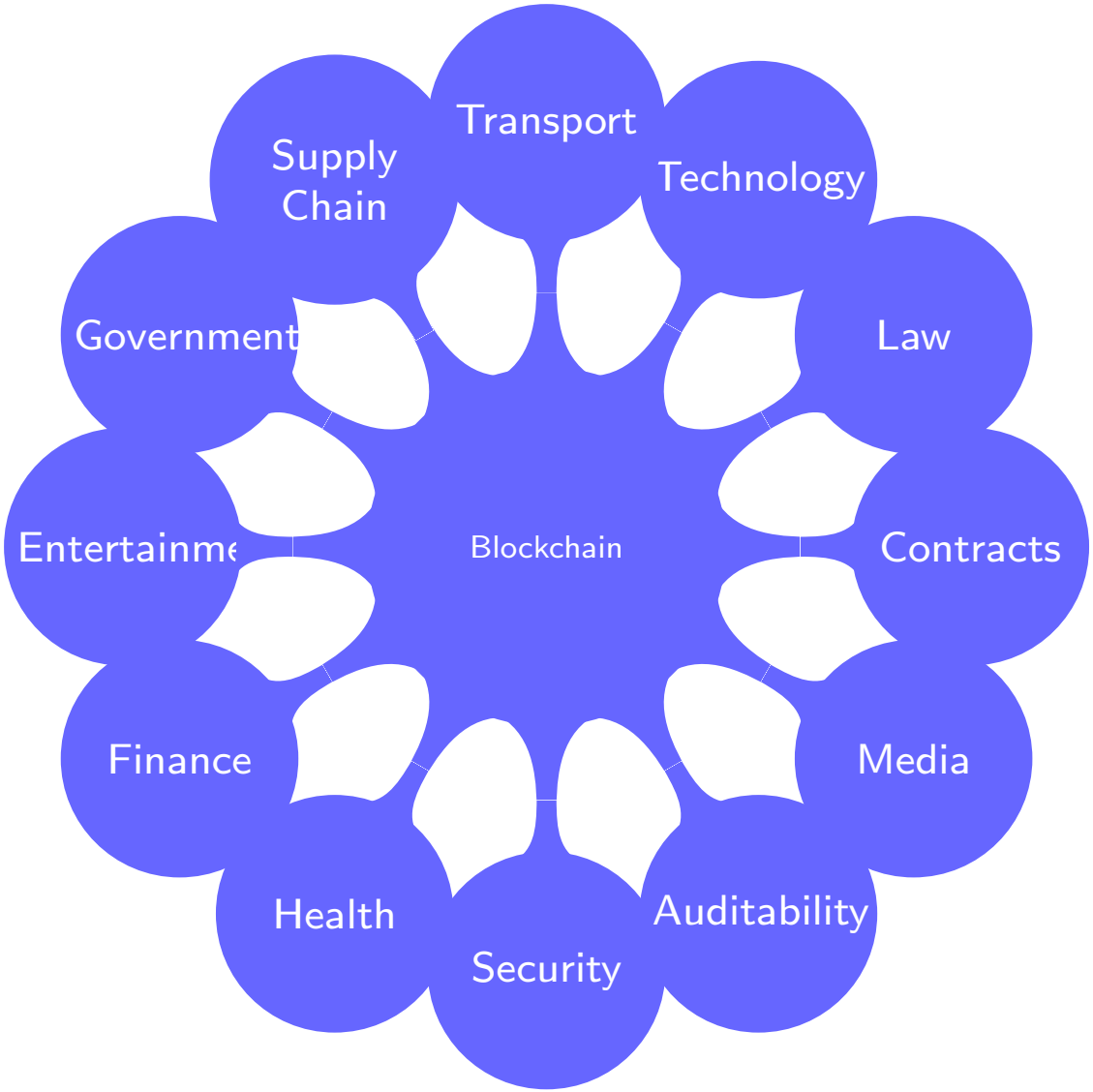
- Finance
  - Loans
  - Finance
  - Business
  - Reduce Uncertainty

Blockchain Mindmap



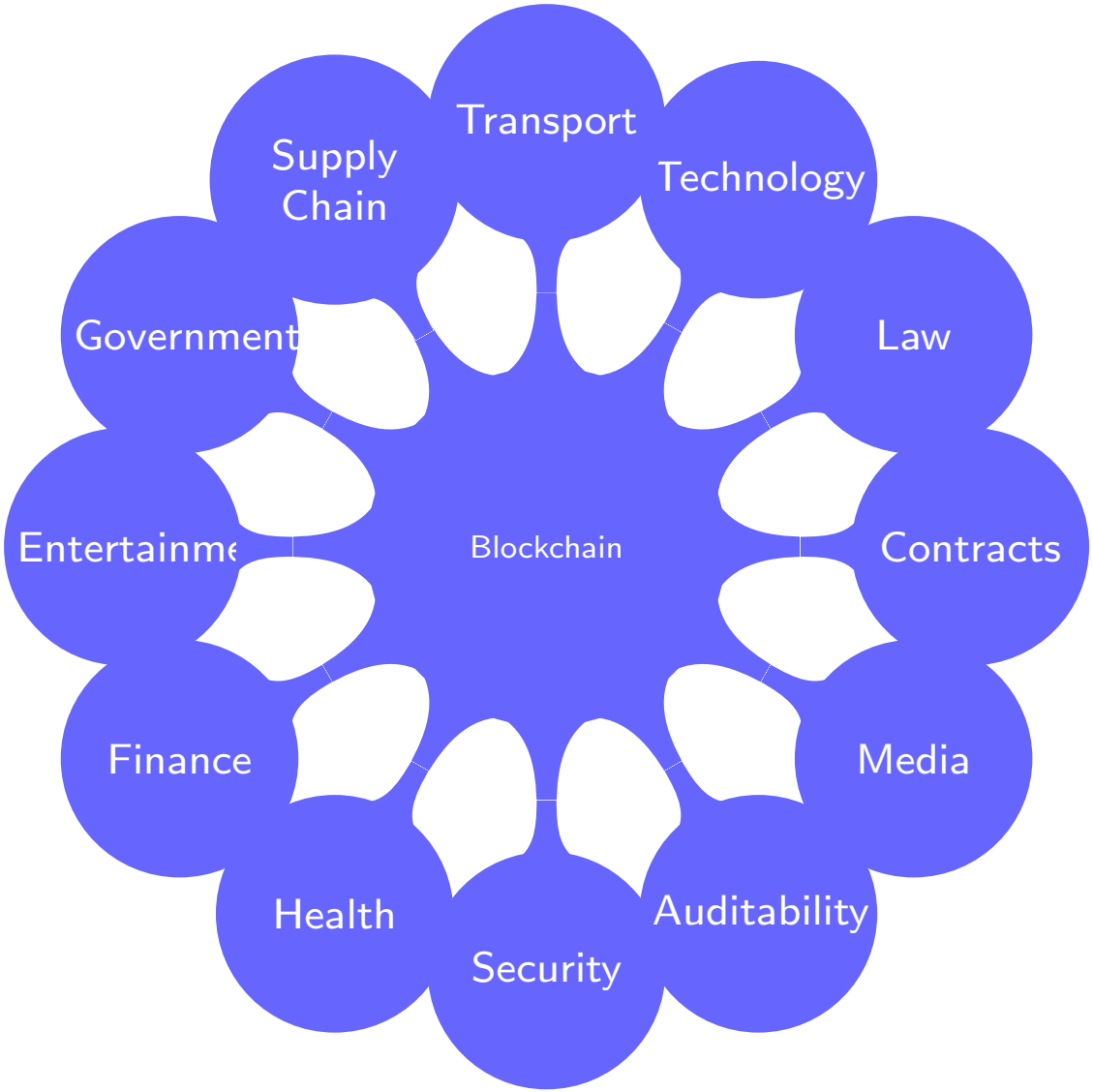
- Health
  - Patient records
  - Patient data
  - Management and RTW
  - Private Health sector

Blockchain Mindmap



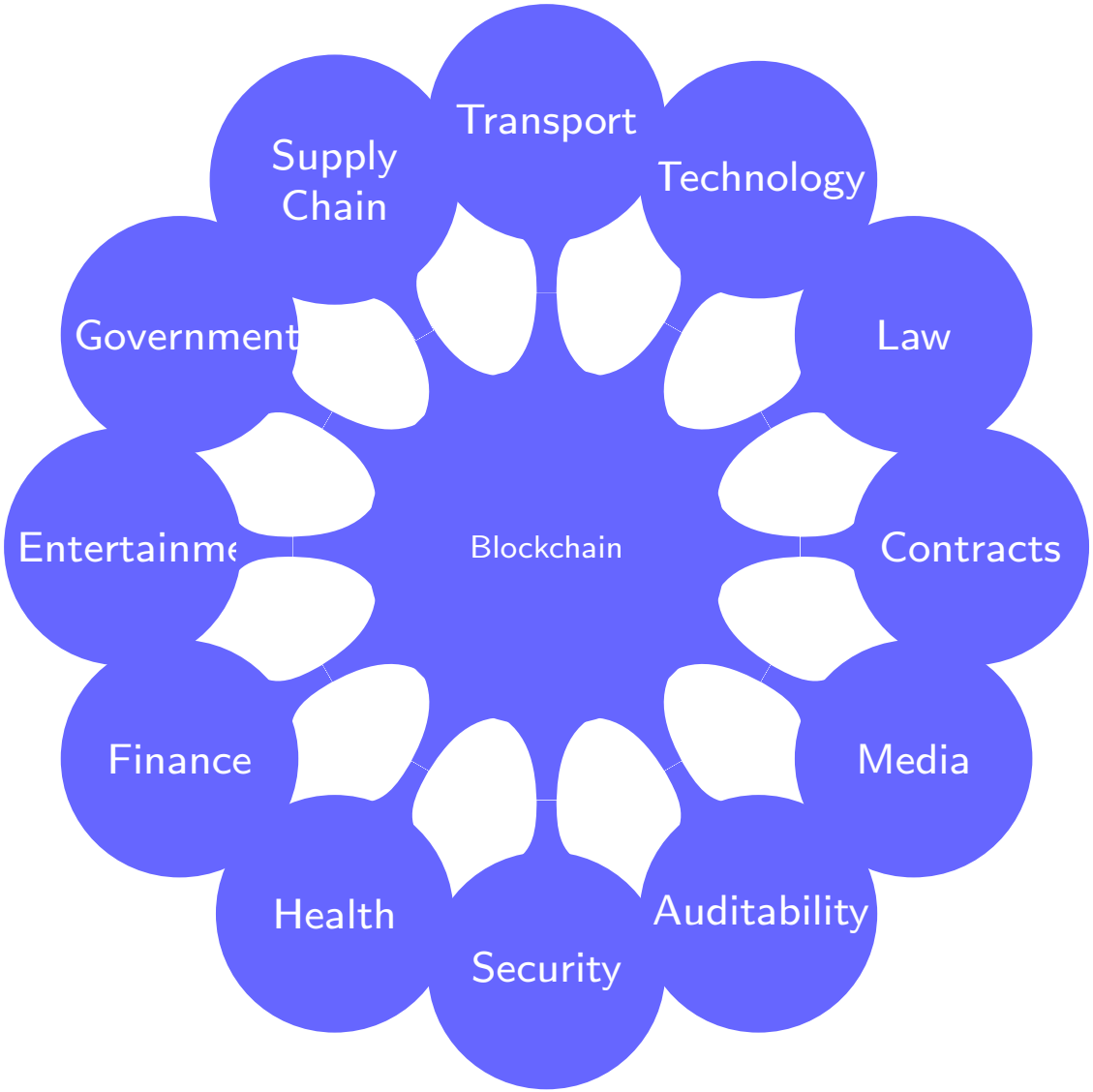
- Security
  - blockchain GB
  - P2P
  - 4K nodes
  - 51% attack

Blockchain Mindmap



- Auditability
  - UK has many audits
  - ISO
  - QAA - universities
  - CQC - healthcare

Blockchain Mindmap



- Media
  - Business
  - share information
  - immutable history

When?

- ₿- BitCoin [3] 2008
- Merkle Trees
- Distributed Ledger Technology
- Hash algorithms
- Crytography
- P2P
- Consensus Algorithms

How and Why?

- How, is what CST4025 is all about
- Why, is a little trickier
- `https://www.youtube.com/watch?v=RplnSVTzvnU`
- Reduce uncertainty
- Motivation

How and Why?

- How, is what CST4025 is all about
- Why, is a little trickier
- `https://www.youtube.com/watch?v=RplnSVTzvnU`
- Reduce uncertainty
- Motivation
  - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

How and Why?

- How, is what CST4025 is all about
- Why, is a little trickier
- `https://www.youtube.com/watch?v=RplnSVTzvnU`
- Reduce uncertainty
- Motivation
  - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
  - "Throughout history, institutions have been divised by human beings to create order and reduce uncertainty in exchange" [4]

How and Why?

- How, is what CST4025 is all about
- Why, is a little trickier
- `https://www.youtube.com/watch?v=RplnSVTzvnU`
- Reduce uncertainty
- Motivation
  - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
  - "Throughout history, institutions have been divised by human beings to create order and reduce uncertainty in exchange" [4]
  - If used correctly blockchain can facilitate the reduction in uncertainty in exchange between institutions.

Blockchain is not *only* Bitcoin

Blockchain $\supset$ Bitcoin

Blockchain

$$\text{Blockchain} \supset \text{Bitcoin}$$

$$\text{Blockchain} \not\equiv \text{Bitcoin}$$

Blockchain

$$\text{Blockchain} \supset \text{Bitcoin}$$

$$\text{Blockchain} \not\equiv \text{Bitcoin}$$

$$\text{Bitcoin} \subset \text{Blockchain}$$

Blockchain Categories [5]

Permissioned

- Private and only authorise users can join
- Access control to blocks, assets and participants
- Authority
- Consensus algorithms are less resource intensive
- tend to be tokenless

Permissionless

- Public and anyone can join
- Read BC
- Write BC
- Malicious users
- Burden on Consensus Algorithms
- tend to be crypto-currency

Blockchain Types [5]

Tokenless

- no cryptocurrency
- information
- transaction
- assets
- participants
- participants exchange information about assets in a transaction

Tokenised

- cryptocurrency
- information
- transaction
- assets
- participants
- participants exchange cryptocurrency in a transaction

Centralised

- Trust
- Governance
- Regulation
- Attributable
- Intermediary
- Transaction Integrity

Building Blocks

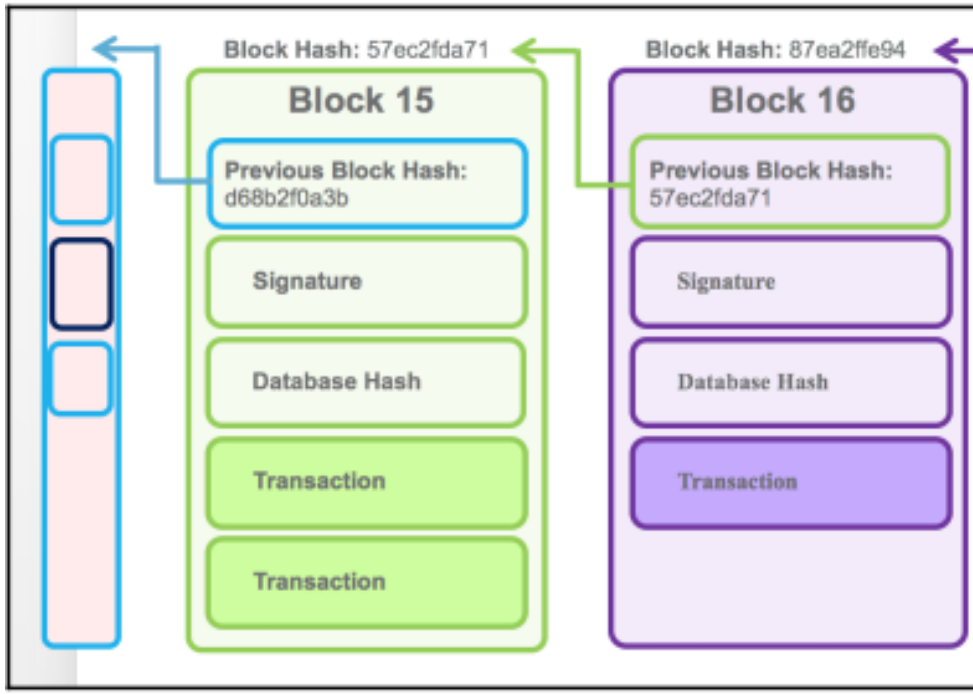
- Shared append only ledger - immutable database
- Cryptography - authentication, integrity & confidentiality
- Consensus - trust and power within the network to verify transactions
- Business Logic or smart contracts - rules component of the transaction, e.g., change ownership, update highest bid, etc...

Other Considerations of blockchain

- Auditability and logging
- Integration: incumbent systems; transaction processing systems;
- Monitoring: quality assurance
- Regulations: compliance
- Authentication: permissioned and authorised

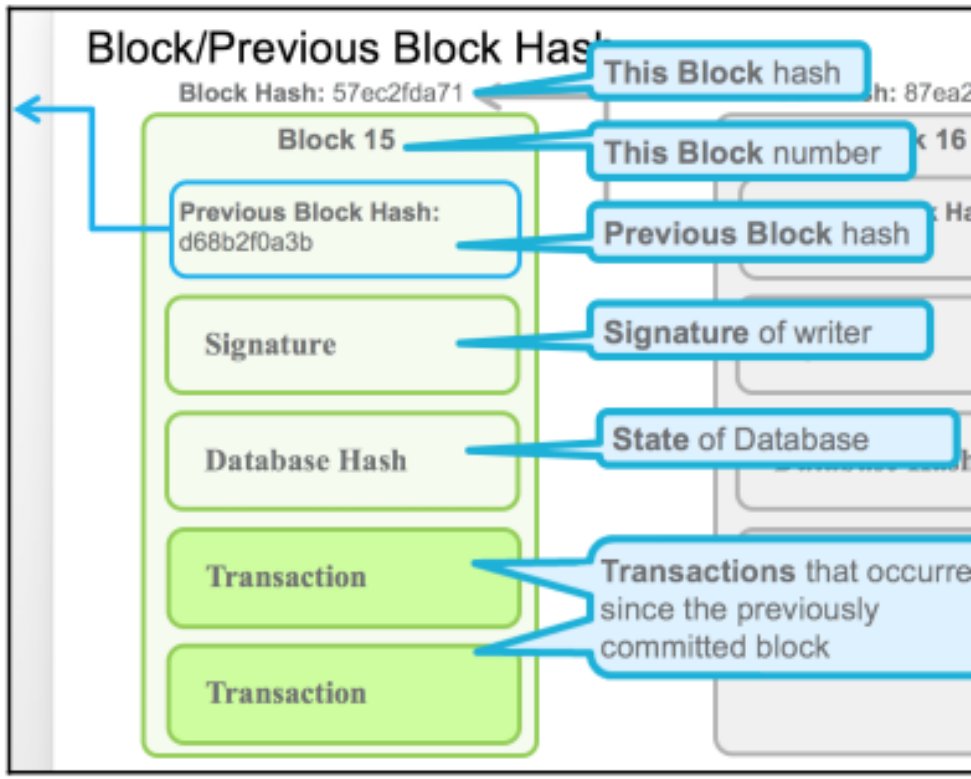
Blockchain Essentials

- Merkle trees
- Hash

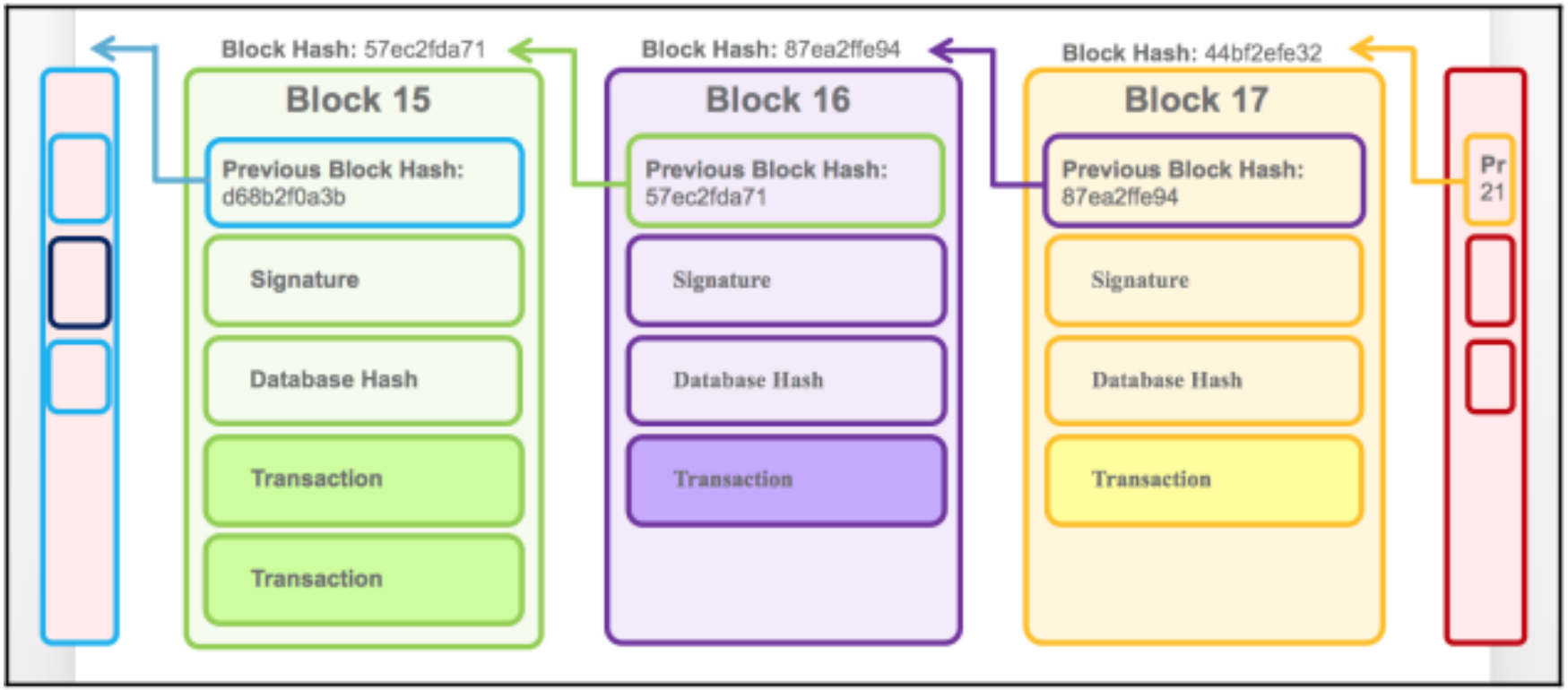


Block Essentials

- Hashes
- Signature
- transaction
- unix timestamp



Blockchain Essentials



Hyperledger Architecture [1]

- Consensus
- Smart Contract
- Communication
- Data Store
- Cryptography
- Policy
- Identity
- API
- Interoperation

Hyperledger Architecture [1]

Consensus

- Verify the correctness of the set of transactions
- A block is composed of multiple transactions
- Concur with other nodes
- Which of these can be trusted?
- Also provides some ordering.
- Consensus algorithm:

Hyperledger Architecture [1]

Consensus

- Verify the correctness of the set of transactions
- A block is composed of multiple transactions
- Concur with other nodes
- Which of these can be trusted?
- Also provides some ordering.
- Consensus algorithm:
  - Confirms the correctness of transactions in a block, according to the consensus algorithms deployed and the policies applied.
  - Once the block is confirmed, then it enters the blockchain, so consensus algorithm has to agree on order the blocks are added
  - Interact and complete smart contract layer

Summary

Blockchain

- P2P
- DLT
  - append-only
  - immutable
  - hash
  - signature
  - blockchain
  - timestamp
- decentralised
- trust

Reading

- NIST [5]
- Hyperledger [1, 2]
- Blockchain TED talk by Bettina Warburg (in slides)

References I

[1] *Hyperledger Architecture, Volume 1*. 2017.

[2] *Hyperledger Architecture, Volume 2*. 2018.

[3] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: (2008).

[4] Douglass C North. "Institutions". In: *Journal of economic perspectives* 5.1 (1991), pp. 97–112.

[5] Dylan Yaga et al. *Blockchain technology overview*. Tech. rep. National Institute of Standards and Technology, 2018.

Web Resources

- `http://hyperledger.org`