CST4125: Blockchain Development
Week: 1
Title: Introduction to Web3.0

Dr Ian Mitchell

smerf.net
Bedfordshire,
UK

2023

Staff Etiquette

Academics

- Record
  - Chatrooms
  - Live
  - Attendance
- Mute control
- Access control
- No anonymity
- Share personal information via screen shares

Student Etiquette

Do's

- Behave as normal, be respectful
- No anonymity
- First and last names to identify you
- Kindness/Difficulty
- Be patient, some one may have technical issues
- Mute microphone, unless speaking
- Use chatroom appropriately
- Keep video on, especially when talking
- Tolerance

Don'ts

- Share personal information
- Try not to multi-task
- Behave inappropriately
- Bully other students
- Disruption
- No eating

Labs

- Complete exercise together
- All leave room
- Try exercise
- Have questions or queries
- Enter waiting room for 1-2-1

Module Aims

Aims

Cover all aspects of the blockchain development lifecycle, which include:

- design and development of blockchain applications;
- applicability of blockchain solutions to I.T. problems;
- evaluation and analysis of blockchain applications; and,
- a comprehensive understanding of specific blockchain technologies.

Module Objectives

Knowledge

On successful completion of this module, the student will be able to:

1. Conceive and assemble decentralised applications as solutions to domain specific problems;
2. Determine and explain components essential to complete a blockchain transaction; and
3. Appraise different components of blockchain technology and determine the applicability of a blockchain solution to a given problem.

Skills

On successful completion of this module, the student will be able to:

1. Exploit a range of techniques to develop and design effective decentralised applications; and
2. Orchestrate a range of techniques to evaluate and analyse

Help

- Library: https://unihub.mdx.ac.uk/study/library
- Space: https://libguides.mdx.ac.uk/bookings
- Laptops: https://unihub.mdx.ac.uk/study/it/laptops-for-loan
- Academic Writing: https://unihub.mdx.ac.uk/study/writing-numeracy/awl-support
- Academic Writing: https://unihub.mdx.ac.uk/study/writing-numeracy/awl-resources
- IT issues: https://unihub.mdx.ac.uk/study/it
- Disability and Dyslexia Service: https://unihub.mdx.ac.uk/support/disability-and-dyslexia
- Mental Health: https://unihub.mdx.ac.uk/support/counselling-and-mental-health
- Welfare: https://unihub.mdx.ac.uk/support/fees-payments-funding
- Changing the Culture: https://unihub.mdx.ac.uk/support/changing-the-culture
- Support: https://unihub.mdx.ac.uk/support

Module Syllabus

CST4125: Syllabus

- Blockchain Anatomy
- Enterprise Blockchain Development
- Cryptocurrency Development
- Smart Contracts, Disintermediation and Decentralised Autonomous Organisations
- Taxonomy of Blockchain Technology
- Consensus Algorithms and Practical Byzantine Fault Tolerance
- Review of Cryptography (PGP)
- Deterministic and Asynchronous programming
- Access Control (RBAC and ABAC)
- Modelling for blockchain (UML)
- Blockchain applicability study

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. Tutor will ask you to wait and you will be invited to join the session at a time suitable so as not to interrupt the learning of others.

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.

CST4125– Indicative Lecture Plan.

Weeks 1-12

Week	Title
1	Web3.0 & Cryptographic Hash Algorithms
2	Data Modelling
3	Access Control
4	Review
5	Introduction to Asynchronous Programming
6	Composer: Transactions
7	Composer: Arrays & Promises
8	Removal Transactions
9	Queries
10	Consensus Engineering
11	Smart Contracts
12	Formative Feedback

Table: Lecture Plan, these are indicative titles

CST4125– Indicative Lecture Plan.

Weeks 13-24

Week	Title
13	Cryptocurency
14	Web-based Wallets
15	Solidity: An Introduction
16	Solidity OOP
17	OOP & Private Networks
18	Evaluation & Testing
19	Security
20	ERC, EIP & Tokens
21	React
22	Case Study
23	Formative Feedback
24	Formative Feedback

Table: Lecture Plan, these are indicative titles

Administration

Assessment

- 100% coursework
  - Coursework 1 (50%)
  - Coursework 2 (50%)
- Formative Feedback: LW11-12
- e-submission for Coursework 1 & 2
- comply to template

Structure

- Attendance $> 75\%$
- Resit: 14^{th} August 2023
- Deferral: 14^{th} August 2023
- Office: TG10
- Teaching:24 * 2 hour Lab; 24 * 1 hour lecture; 9.5 hours independent study
- Mitigating circumstances: see unihelpdesk and apply for deferral

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: smerf.net

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: smerf.net

Office Hours

- During term time only
- When: Winter Term: Mondays 1100-1300hrs
- Please read notifications or emails
- There are occassions that these could be arranged online, e.g., due to industrial action or inclement weather

Deadlines

				Feedback	
Description	Submission	Weight	Deadline	Formative	Summative
1. Hyperledger	MyLearning	50%	14th April 2023	LW11-12	10/05/2023
2. Ethereum	MyLearning	50%	8th July 2023	LW23-24	28/07/2023
Resits	MyLearning	50-100%	14th August 2023	None	None
Deferals	MyLearning	50-100%	14th August 2023	None	None

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?

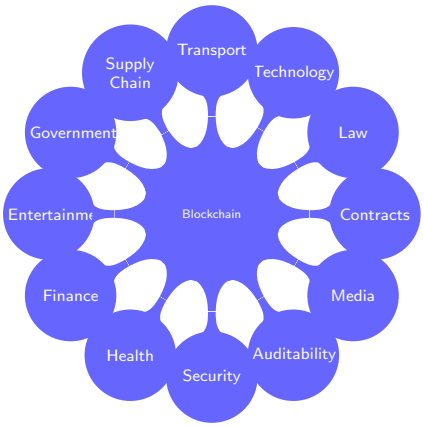
Blockchain Definition

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

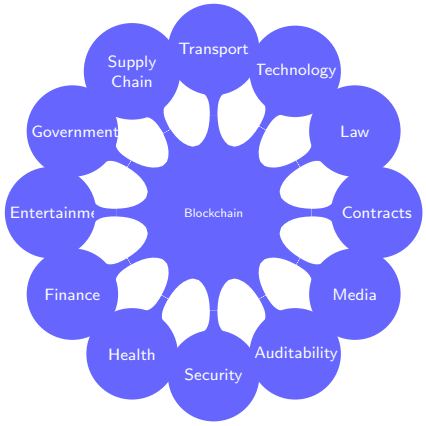
- Decentralised
- Consensus
- P2P
- Blockchain
- Cryptography
- Blockchain [1]

[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?

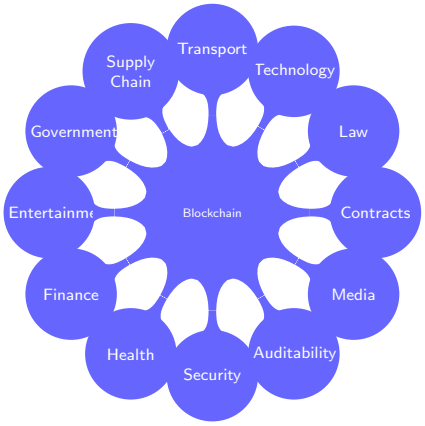


Blockchain Mindmap



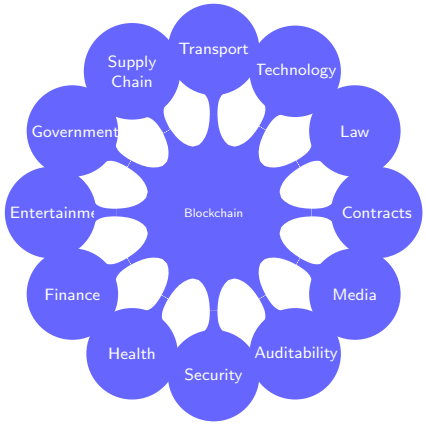
- Contracts
  - Smart Contracts
  - Release payment upon satisfying contractual obligations
  - Ratified by using blockchain

Blockchain Mindmap



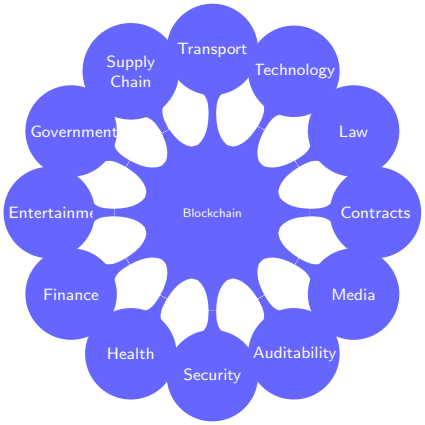
- Law
  - restriction on dangerous items, e.g. gun control
  - Police procedures

Blockchain Mindmap



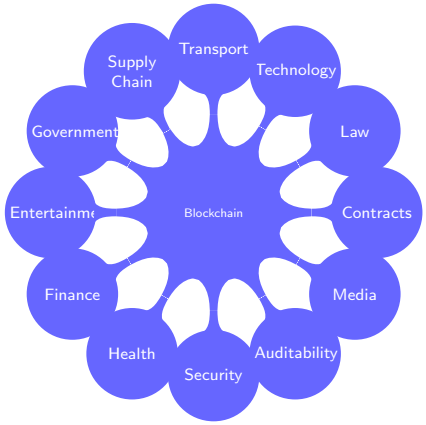
- Technology
  - All areas are seeing blockchain involvement
  - Fridges, Washing machines, smart environments
  - Cyber Security
  - Cloud Storage
  - Internet of Things, IoT

Blockchain Mindmap



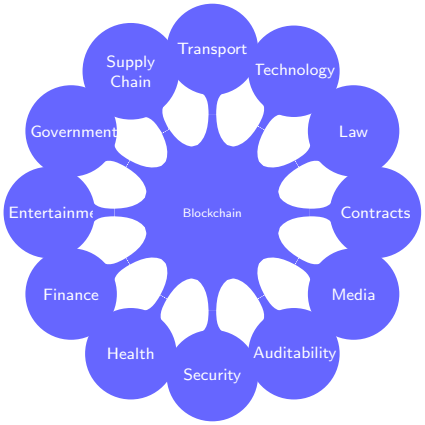
- Transport
  - Public Transportation
  - Automotive
  - Business - fleets of vehicles and navigation

Blockchain Mindmap



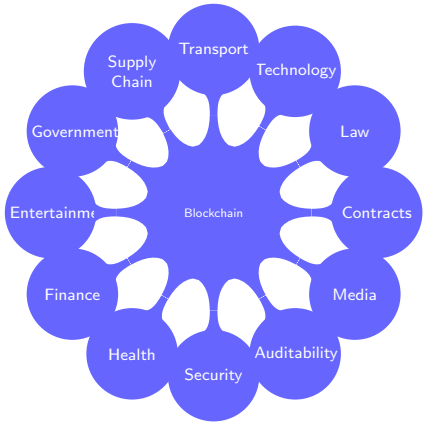
- Supply Chain
  - JIT delivery
  - Pre-conditions
  - Smart contracts
  - Secure
  - Third party
  - Mutual (dis)trust

Blockchain Mindmap



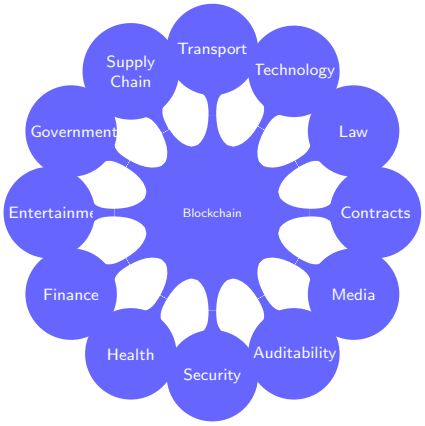
- Government
  - ID Management
  - Electoral
  - Tax

Blockchain Mindmap



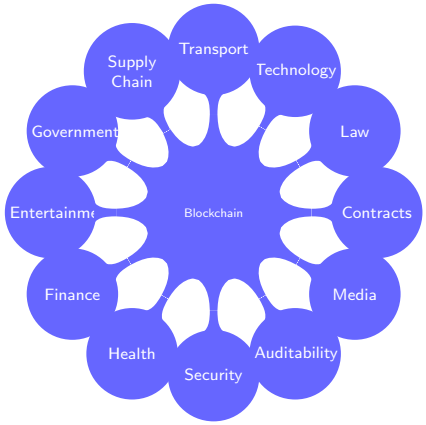
- Entertainment
  - Copyright
  - Digital Rights

Blockchain Mindmap



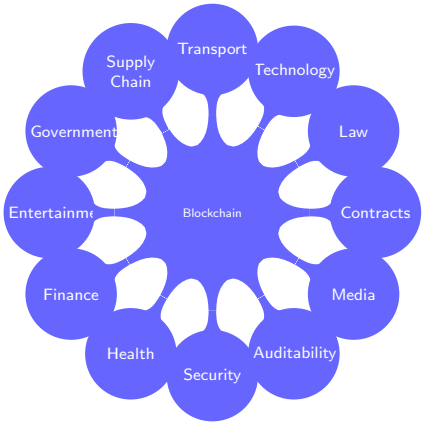
- Finance
  - Loans
  - Finance
  - Business
  - Reduce Uncertainty

Blockchain Mindmap



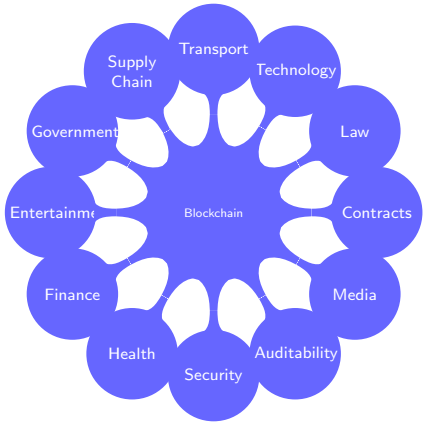
- Health
  - Patient records
  - Patient data
  - Management and RTW
  - Private Health sector

Blockchain Mindmap



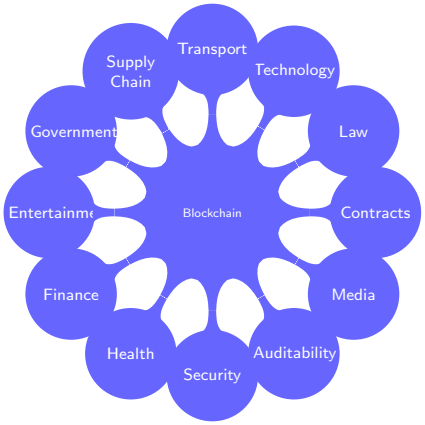
- Security
  - blockchain GB
  - P2P
  - 4K nodes
  - 51% attack

Blockchain Mindmap



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

Blockchain Mindmap



- Media
  - Business
  - share information
  - immutable history

When?

- ₿- BitCoin [**nakamoto2008bitcoin**] 2008
- Merkle Trees
- Distributed Ledger Technology
- Hash algorithms
- Cryptography
- P2P
- Consensus Algorithms

How and Why?

- How, is what CST4125 is all about
- Why, is a little trickier
- `https://www.youtube.com/watch?v=RplnSVTzvnU`
- Reduce uncertainty
- Motivation

How and Why?

- How, is what CST4125 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 CST4125 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" [**north1991institutions**]

How and Why?

- How, is what CST4125 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" [**north1991institutions**]
  - If used correctly blockchain can facilitate the reduction in uncertainty in exchange between institutions.

Blockchain

Blockchain is not *only* Bitcoin

Blockchain

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

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 [**yaga2018blockchain**]

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 [**yaga2018blockchain**]

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

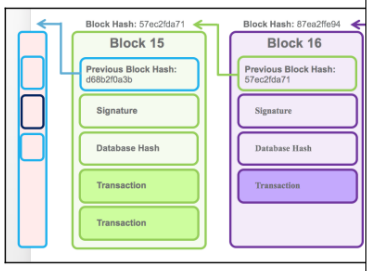
- Shared append only ledger - immutable database
- Cryptography - authentication, integrity & confidentiality
- Consensus - trust and power within the network to verify transactions
- Business Logic or smart contracts - rules component of the transaction, e.g., change ownership, update highest bid, etc...

Other Considerations of blockchain

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

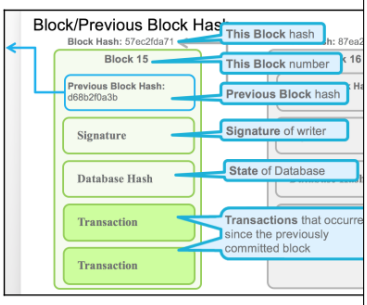
Blockchain Essentials

- Merkle trees
- Hash



Block Essentials

- Hashes
- Signature
- transaction
- unix timestamp



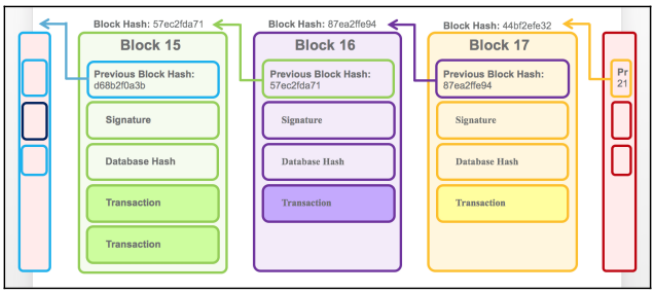
Hash Algorithms

- Ethereum uses Keccak-256
- NIST recommends
- Unique
- Input: any size
- Ouput: fixed size

Properties

1. **Pre-image Resistant**: Computationally infeasible to calculate x, given $H(x)$.
2. **Second Pre-image Resistant**: Computationally infeasible to find an input that hashes to a specific output. Given x find y s.t. $H(x) = H(y)$
3. **Collision Resistant**: Two inputs that hash to the same output. Find x and y s.t. $H(x) = H(y)$

Blockchain Essentials



Hyperledger Architecture [**hyperledger:1**]

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

Hyperledger Architecture [**hyperledger: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 [**hyperledger: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 [**yaga2018blockchain**]
- Hyperledger [**hyperledger:1**, **hyperledger:2**]
- Blockchain TED talk by Bettina Warburg (in slides)

References I

Web Resources

- `http://hyperledger.org`