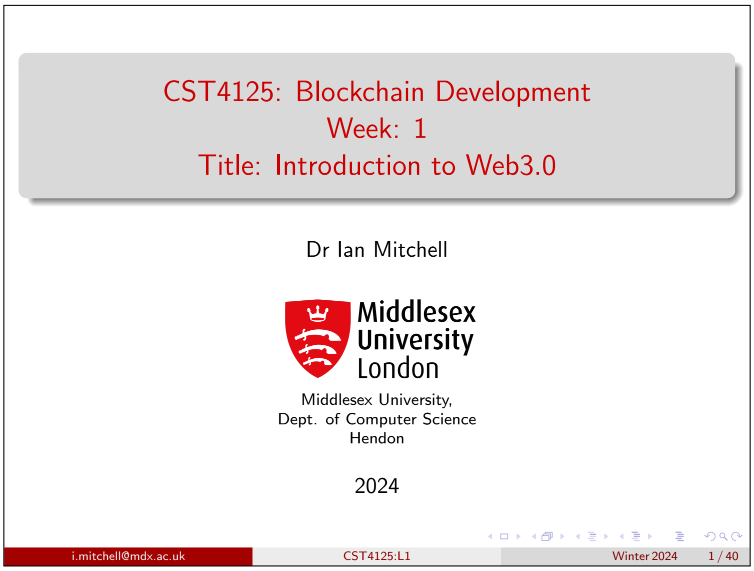
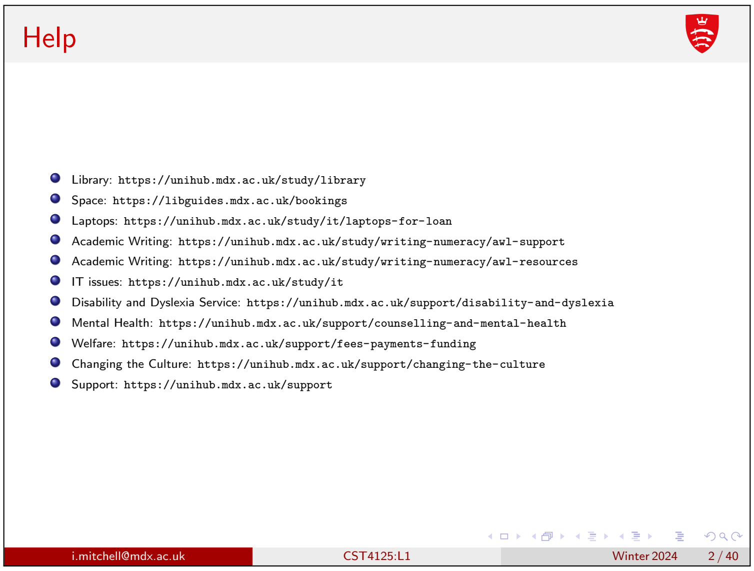


CST4125: Blockchain Development
Week: 1
Title: Introduction to Web3.0

Dr Ian Mitchell

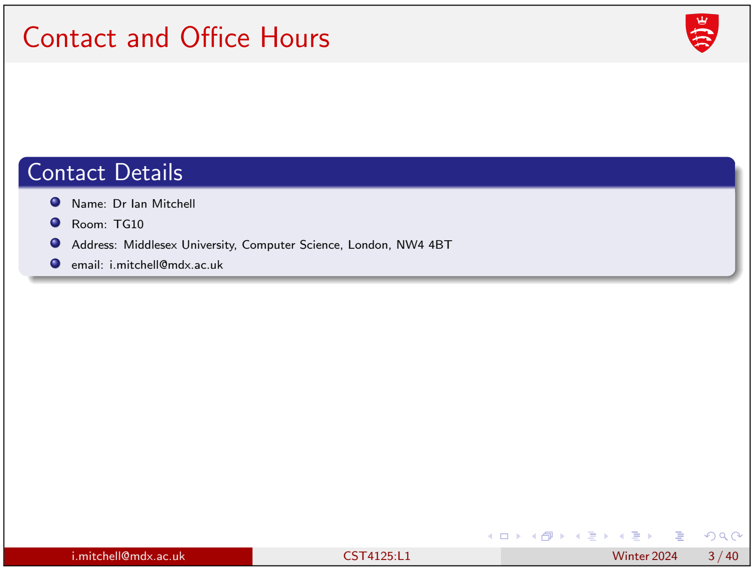
Middlesex University,
Dept. of Computer Science
Hendon

2024



Help

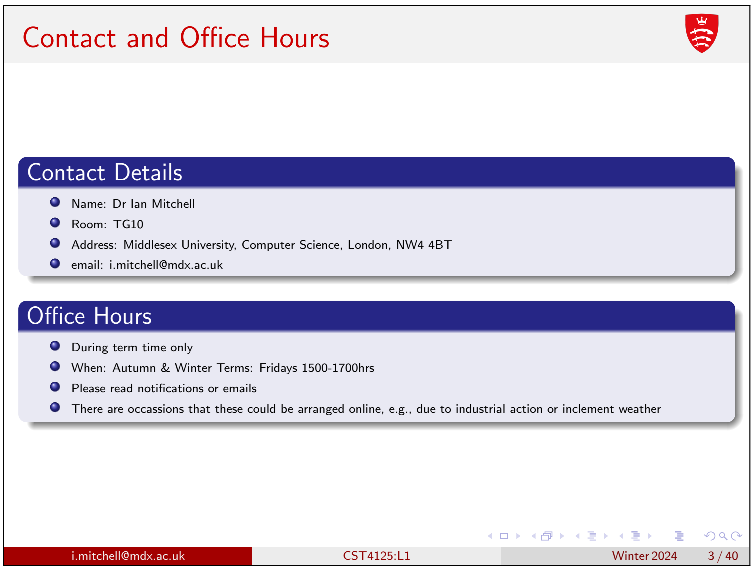
- Library: `https://unihub.mdx.ac.uk/study/library`
- Space: `https://libguides.mdx.ac.uk/bookings`
- Laptops: `https://unihub.mdx.ac.uk/study/it/laptops-for-loan`
- Academic Writing: `https://unihub.mdx.ac.uk/study/writing-numeracy/awl-support`
- Academic Writing: `https://unihub.mdx.ac.uk/study/writing-numeracy/awl-resources`
- 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`



Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: i.mitchell@mdx.ac.uk



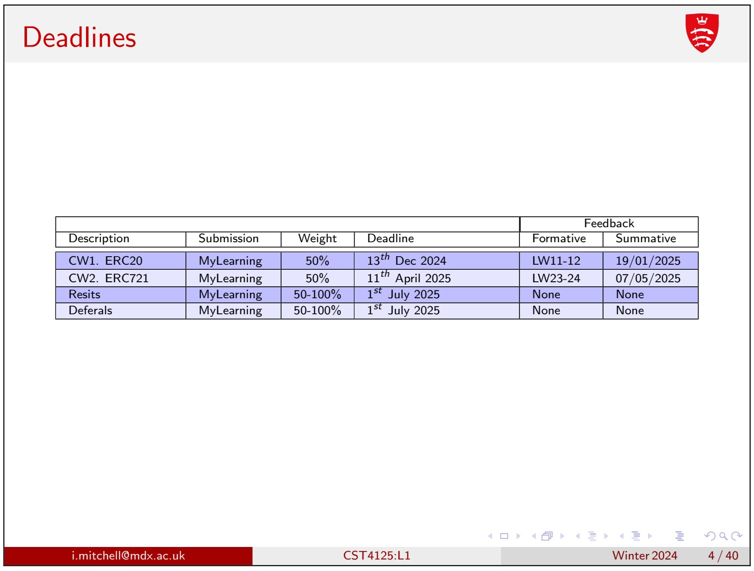
Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: i.mitchell@mdx.ac.uk

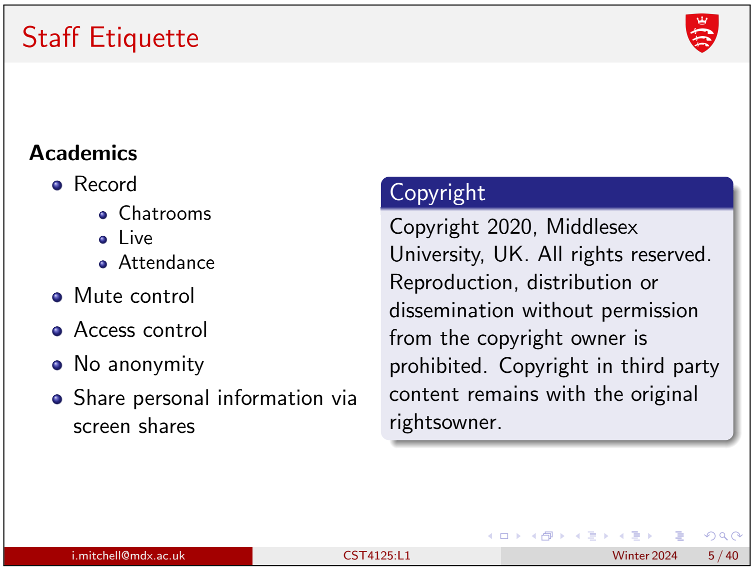
Office Hours

- During term time only
- When: Autumn & Winter Terms: Fridays 1500-1700hrs
- 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
CW1. ERC20	MyLearning	50%	13th Dec 2024	LW11-12	19/01/2025
CW2. ERC721	MyLearning	50%	11th April 2025	LW23-24	07/05/2025
Resits	MyLearning	50-100%	1st July 2025	None	None
Deferals	MyLearning	50-100%	1st July 2025	None	None



Staff Etiquette

Academics

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

Copyright

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 decentralised applications

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, ERC-20

Week	Description
1	Blockchain Anatomy: Yaga's Paper. Permissioned v. Permissionless
2	Consensus Engineering/Algorithms: Proof of Stake; Proof of Elapsed-Time; Proof of Work; others
3	Smart Contracts: EVM; Dapps; Purpose; Use Case; BitCoin & Ethereum differ; Ethereum Yellow Paper
4	Ethereum: Introduction to my first contract; solidity; addresses; wallets; faucets;
5	Ethereum: Solidity: addresses, mappings, data structures, enum, time, reference v. value
6	Ethereum: Solidity: function modifiers, class structure, fallback, receive, OOP, conditions
7	Security: Reentrancy; Overflow; Underflow; padding of address
8	ERC20: transfer from and tokens
9	ICO for ERC20: create simple ico and transfer tokens
10	Unit testing: chai, hardhat, cli, vscode
11	Testing with hardhat
12	Case Study and putting it all together

CST4125– Indicative Lecture Plan.

ERC-721

Week	Title
13	Node.js: asynchronous programming; arrow functions; await;
14	React:npm, elements, bulma/css, properties
15	React: state, effect and hooks
16	React, wallets & web3
17	React, wallets & ether.js
18	React, wallets & wagmi
19	NFT: ERC721, & ERC1155
20	React and ERC721
21	Other ERCs Coincidence of Want (CoW) 1271, multi-sig, Maximal Extractable Value, frontrunning protection
22	User onboarding: Signatures, Meta-transactions (EIP712), Indexing
23	Current Research and the future of Blockchain and Other Networks
24	Case Study

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: 1st July 2025
- Deferral: 1st July 2025
- Office: TG10
- Teaching:24 * 2 hour Lab; 24 * 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 distributed ledger forged via consensus on a Peer-to-peer (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?

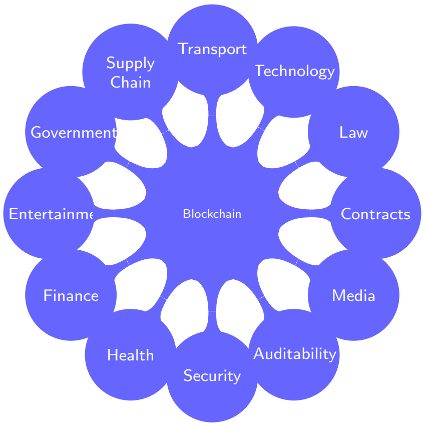
Blockchain Definition

Append-only immutable distributed 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?



When?

- ₿- BitCoin [2] 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" [3]

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" [3]
  - If used correctly blockchain can facilitate the reduction in uncertainty in exchange between institutions.

Blockchain

Blockchain is not *only* Bitcoin

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

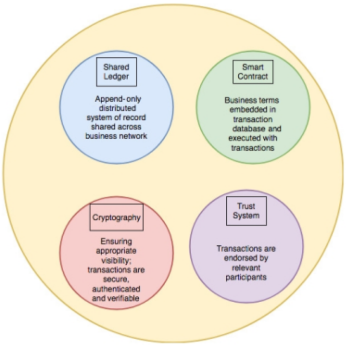
- cryptocurrency
- information
- transaction
- assets
- participants
- participants exchange cryptocurrency in a transaction

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...

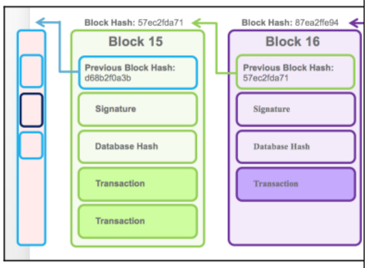

Shared Ledger
Append-only distributed system of record shared across business network
Smart Contract
Business terms embedded in transaction database and executed with transactions
Cryptography
Ensuring appropriate visibility; transactions are secure, authenticated and verifiable
Trust System
Transactions are endorsed by relevant participants

Other Considerations of blockchain

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

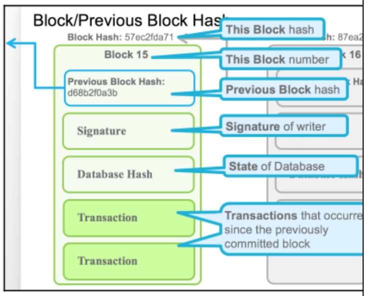
Blockchain Essentials

- Merkle trees
- Hash



Block Essentials

- Hashes
- Signature
- transaction
- unix timestamp



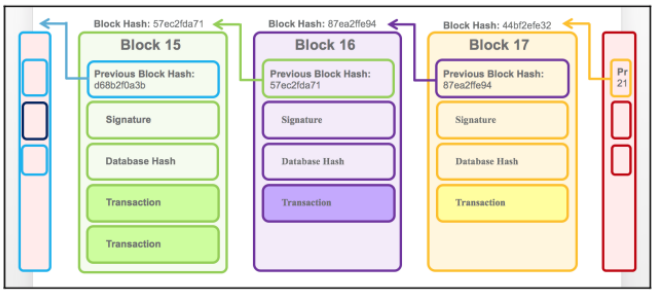
Hash Algorithms

- Ethereum uses Keccak-256
- National Institute of Standards and Technology (NIST) recommends
  - Computer Security Resource Center
- 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



Applicability

- Not same as AI
- Not same as most software development
- Many frameworks blockchain applicability
- Is what I am developing fit for purpose?

Scriber [4]

- 2016 Development $1.4Bn
- Check, confirm and accept
- Distributed, ordered, back-linked list of blocks
- Trust creation and consensus
- Wide and varied.
- Database?

Blockchain appropriateness

- Immutability
- Visibility & Transparency
- Trust
- Identity
- Distribution
- Workflow
- Transactions
- Historical Records
- Inefficiency

Evaluation

Characteristic	W	%	W*%
Immutability	12	_	_
Transparency	12	_	_
Trust	16	_	_
Identity	5	_	_
Distribution	10	_	_
Workflow	5	_	_
Transactions	12	_	_
Historical Record	8	_	_
Ecosystem	15	_	_
Inefficiency	5	_	_
Total	100	_	_

Table: Form for evaluation of blockchain applicability, [4]

Applicability

Question	Considerations
Will this project require updates, mutability, or deletion of records?	Blockchains are inherently permanent. If the architecture requires anything other than rare addtions of new blocks to invalidate prior blocks, the overhead of checking for revocations can have a significant negative impact in mature or large chains.
Is there agreement that all blockchain participants should be able to view and validate transaction details?	Disitribution of blockchains and validation of transactions are crtical. Without the use of obfuscating techniques that allow for transaction validation without viewing, the power of distributed trust in the chain world would be lost to the sing node that oringinally validated the transaction, which might not even be a permanent member of the chain.

Table: Criteria of blockchain applicability, [4]

Applicability

Question	Considerations
Does this architecture fit well in an ecosystem of diverse participants?	For internal projects in which significant trust already exists, a database solution will likely be far more economically appropriate.
Are the adequate incentives for participants to continue to support the chain indefinitely?	From the economic and technical perspectives, support for the chain's future depends on the maintenance of that chain and storage of previous blocks

Table: Criteria of blockchain applicability, [4]

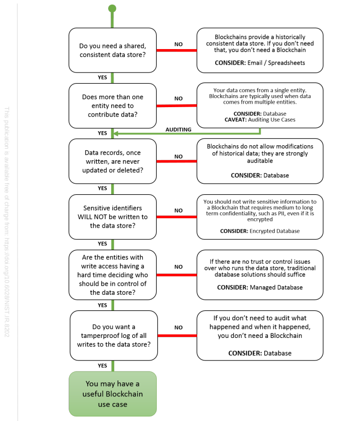
Applicability

Question	Considerations
From and efficiency perspective, are there enough participants and sufficient complexity to buoy the consensus model, validate all transactions, and approve the authentication and authorization processes?	Here, the economic and techinical considerations collide when you consider not only the long-term power, computation, backup, maintenance, and support requirements but also the changing landscape of adversarial engineering. Will the chain continually have enough positive influence in the consensus model to counteract negative actors and achieve Byzatine fault tolerance.

Table: Criteria of blockchain applicability, [4]

NIST [5]

NISTIR 8202 BLOCKCHAIN TECHNOLOGY OVERVIEW



Do you need a shared, consistent data store?

NO

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

CONSIDER: Email / Spreadsheets

YES

Does more than one entity need to contribute data?

NO

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.

CONSIDER: Database

CAVEAT: Auditing Use Cases

AUDITING

YES

Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

CONSIDER: Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

CONSIDER: Encrypted Database

YES

Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

CONSIDER: Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don't need to audit what happened and when it happened, you don't need a Blockchain

CONSIDER: Database

YES

You may have a useful Blockchain use case

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8202

Figure 6 - DHS Science & Technology Directorate Flowchart

Other considerations

- Everything is automated/digitised
- Disintermediation
- Auditing
- Trust
- Tokens - Incentivisation
- Cryptocurrencies are part of Blockchain
- Permissioned/Permissionless
- Smart Contracts

Summary

Blockchain

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

Reading

- NIST [5]
- Gourisetti *et al* [1]
- Blockchain TED talk by Bettina Warburg (in slides)
- Scriber [4]

Web Resources

- hyperledger
- Ethereum
- Web3.0 Foundation

References I

[1] Sri Nikhil Gupta Gourisetti, Michael Mylrea, and Hirak Patangia. "Evaluation and demonstration of blockchain applicability framework". In: *IEEE Transactions on Engineering Management* 67.4 (2019), pp. 1142–1156.

[2] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Nakamoto Institute. [Accessed: Jan 2022]. 2008.

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

[4] Brian A Scriber. "A framework for determining blockchain applicability". In: *IEEE Software* 35.4 (2018), pp. 70–77.

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

Glossary

ERC Ethereum Request for Change. 12, 13

NIST National Institute of Standards and Technology. 32

P2P Peer-to-peer. 16, 17, 19