

Blockchain Technology and Applications

CS 731

Blockchain technology

Dr. Ir. Angshuman Karmakar

IIT Kanpur

Teaching assistants

- **Sumit Lahiri** (sumitl@cse.iitk.ac.in)
- **Chavan Sujeet** (sujeetc@cse.iitk.ac.in)
- **Indranil Thakur** (indra@cse.iitk.ac.in)

Broad perspective

- What is blockchain?
- Evolution of Blockchains.
- Fundamental components of blockchains
- Types of blockchains
- What is cryptocurrency?
 - How do real-world cryptocurrencies such as Bitcoin, Ethereum, etc. work.
- Advantage and disadvantages of cryptocurrencies etc.
- What we are not going to learn
 - Trading
 - ICO
 - Or anything related to real-world finance
- **Disclaimer: All discussions are for academic interest only**

Why a course on Blockchain?

- In the news lately
 - Bitcoin
 - Ethereum
 - Blockchain for E-governance
 - Blockchain for supply chain management
 - Blockchain for energy management
- Is it just a hype and hyperbole?
 - Hopefully this course will teach you otherwise
 - Even if you do not care about cryptocurrency and its market volatility
 - Blockchain has lots of other applications

What is Blockchain?

- A means to store data
 - Distributed: across multiple nodes or computing devices
 - Decentralized: No central authority
 - Replicated: identical copies in many nodes
 - Immutable: once committed can't be changed
 - Guaranteed by cryptography
 - Consistent: all nodes in different locations have the same value
 - Consensus mechanism
 - Integrity: content is same as the user intends

What is Blockchain?

- A means to store data
 - Distributed: across multiple nodes or computing devices
 - Decentralized: No central authority
 - Replicated: identical copies in many nodes
 - Immutable: once committed can't be changed
 - Guaranteed by cryptography
 - Consistent: all nodes have same value
 - Consensus mechanism
 - Integrity: content is same as the user intends
- Used for
 - Electronic currency, transactions
 - Tamper resistant log
 - Immutable ledger for transactions (non-currency related)
 - Smart contracts

Applications

Banking (Courtesy Arvind Narayanan)



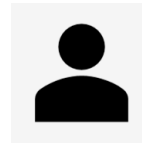
Regulatory Agency (RBI)



Customers



Bank



Bank Employee

How do you transact?

- You write a check or do internet transaction to pay a payee
- Bank checks if you have $\text{balance} > \text{transaction_amount}$
 - If yes, it debits your account by $\text{balance} = \text{balance} - \text{transaction_amount}$
 - credit's payee's account by $\text{payee.balance} = \text{payee.balance} + \text{transaction_amount}$
 - If no, the transaction is invalid and rejected.
- You can check your transaction list online, or check the monthly statement
- Who maintains the ledger?
 - Bank Does
 - What if Bank allows an invalid transaction go through
 - Invalid = you did not authenticate the transaction
 - Invalid = your balance was not sufficient but transaction was made

Bank Frauds

- You find a check was used to pay someone but you never wrote the check
 - Someone forged your check and/or signature
- You did sign a check for x amount, but the amount field was modified
 - How do you prove to the bank that an extra 0 was not there in your signing time?
- The monthly statement says that you did a transaction but you did not recall or the amount of a transaction is different from what you had done
 - Someone got your password, and possibly redirected OTP to another SIM (SIM Fraud)
 - Bank employees themselves might have done something
- How do you argue to the bank? (Non-repudiation)
- How do you argue that the amount was modified? (Integrity)
- Finally, do you tally your transactions when you receive your monthly statement?
 - Most people do not

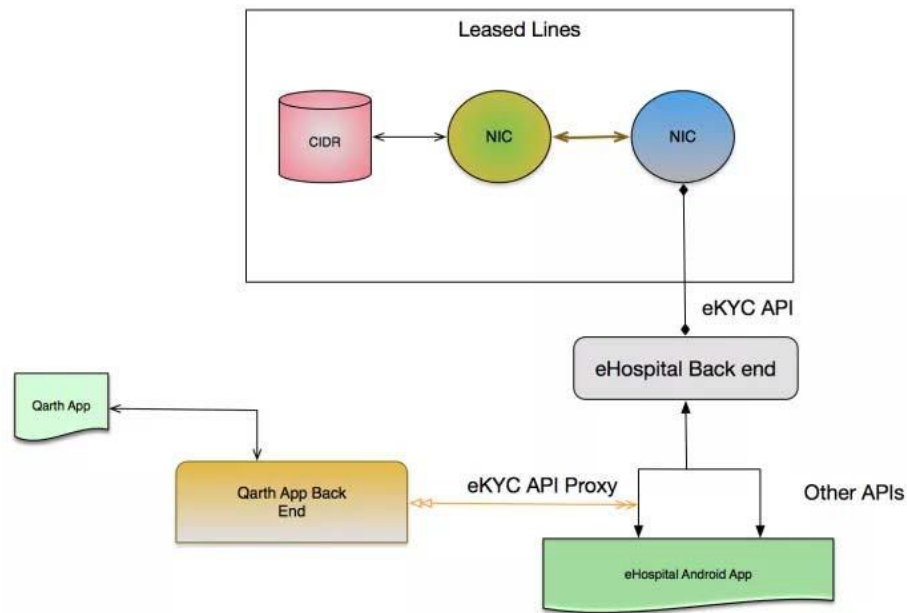
Supply chain and provenance

- Your buy ice cream for your restaurant from supplier B
- Supplier B actually transports ice cream made in Company C's factory
- Upon delivery, you have been finding that your ice cream is already melted
- Who is responsible?
 - Supplier B is keeping it too long on the delivery truck?
 - Supplier B's storage facility has a temperature problem?
 - Supplier C says it's supplier B's fault as when picked up – ice cream was frozen
 - Supplier B says that when received, the temperature was too high, so C must have stored it or made it wrong
 - How do you find the truth?
 - Put temperature sensors in B's truck and storage, C's factory and storage, and sensor data is digitally signed by the entity where the sensor is placed and put in a log
 - You check the log – but B and C both have hacked the log and deleted some entries?
- What to do?

Land Record

- Tampering land record is common in India and many other nations
- You buy a piece of land
- Someone else claims to own the land
- But the one who sold you the land showed you paper work
- Land registry office earlier said that the owner was rightful
- Now they say that they made a mistake – it was owned by the other person
- You already paid for the land – to the first person
- First person goes missing
 - How does any one prove who changed the land record?
 - The government employees?

Then there is Aadhaar

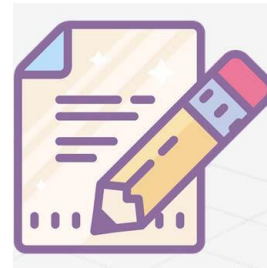


- E-KYC Logs
- Shown to you by UIDAI
- How do you know they did not delete important log events?
- Do you Trust UIDAI?

A student Online Grade Submission and Management System



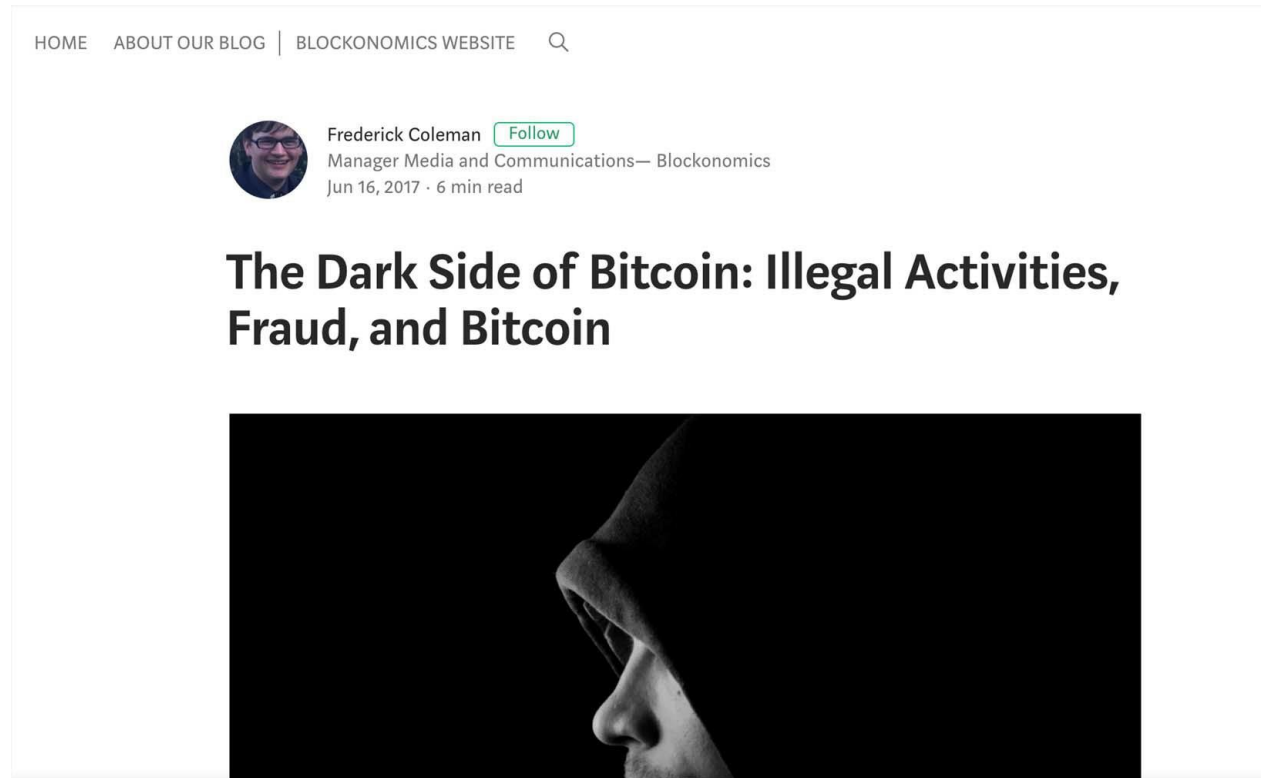
Professor	Course	Grade
1	ESC101	D
2	CS698	D
3	CS425	D
4	CS771	D



This course is not about bitcoin or currency: Why?




Why not bitcoin? (2)



Why not bitcoin? (6)

[Entertainment](#) [Tomorrow](#) [Video](#) [Reviews](#) [Events](#) [US Edition](#)

Entirely predictable...
so you don't have to be.




Get the app

AdChoices

China reportedly wants to curtail wasteful bitcoin mining

It doesn't like the waste and fears a crash would cause economic havoc.



Steve Dent, @stevetdent
01.08.18 in [Business](#)

4
Comments

354
Shares

Why no money business?



Quadriga Exchange – Loss of 145 USD worth cryptocurrency

A crypto exchange may have lost \$145 million after its CEO suddenly died

By Daniel Shane, [CNN Business](#)

Updated 0251 GMT (1051 HKT) February 6, 2019



TOP STORIES



Steve Harvey ha
Miss Universe m



A wildlife conse
mauled by her o

Recomm

Why no money business? (2)



Why no money business? (2)



Join TechCrunch+

Login

Search Q

TechCrunch+

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

More

Crypto

India seizes \$46 million from crypto exchange Vault in money-laundering probe

Manish Singh @refsrc / 6:57 PM GMT+5:30 • August 12, 2022

Comment

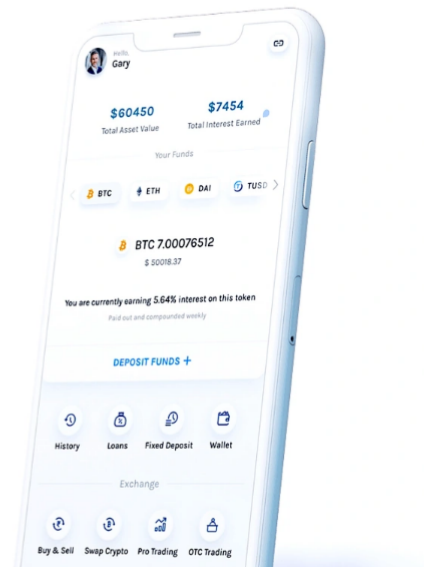



Image Credit: Monda

Why no money business? (2)

INVESTINGSIMULATORBANKINGPERSONAL FINANCENEWSREVIEWSACADEMY

[BUYING & SELLING](#) > [CRYPTO EXCHANGES](#)

The Collapse of FTX: What Went Wrong With the Crypto Exchange?

By [NATHAN REIFF](#) Updated February 27, 2023

Reviewed by [ERIKA RASURE](#)

Fact checked by [VIKKI VELASQUEZ](#)

Cryptocurrency exchange FTX and its founder and former CEO, Sam Bankman-Fried, are intricately entwined. The swift and damaging [collapse of FTX in late 2022](#) will have repercussions on the international crypto community for years to come.

Learn more about what went wrong with FTX.

Table of Contents

- What Happened to FTX?
- FTX Collapse's Sequence of Events
- Arrest, Charges Against Bankman-Fried
- Future of FTX and Consequences of Collapse
- FAQs
- The Bottom Line

Bitcoins and other cryptocurrencies

- Too much interest by investors to park their assets
- Less use as a medium of value exchange
- Private Key stealing or private keys at exchanges — risk
- Coding vulnerabilities — risk
- Volatility
- Energy Waste — climate impact
- Too much concentration in one country — risk
- Regulatory risk
- Usage for criminal activities — Silk Road

Trust Model

- Cyber Security is all about who you trust?
 - Trust your hardware to not leak your cryptographic keys?
 - Trust your O/S to not peek into your computation memory?
 - Trust your hypervisor to not mess up your process memory?
 - Trust your application to not be control hijacked or attack other applications?
- Where is your trust anchor?
 - Hardware?
 - Operating system?
 - Application?
 - Manufacturer?

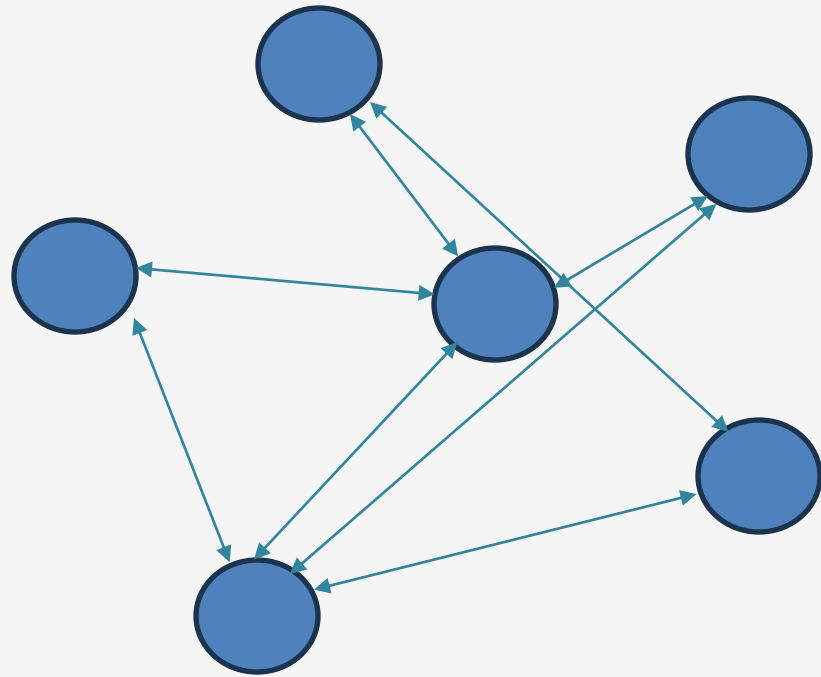
Trust Model (2)

- In many real-life transactional activities – trust model is the inverse of the threat model
 - Do you trust your bank to not take out small amounts from your balance all the time? (Watch – “Office Space”)
 - Do you trust the department of land records to keep your record’s integrity?
 - Do you trust UIDAI officials to keep your aadhaar data from unauthorized access?
 - Do you trust your local system admins to not go around your back and change settings, leak passwords, change database entries, and remove their action from system logs?
 - In the patch management system of your enterprise, are the patches being put -- all have digital certificates? Who put them? Do you trust your employees to do the correct thing and not put a malware as patch?

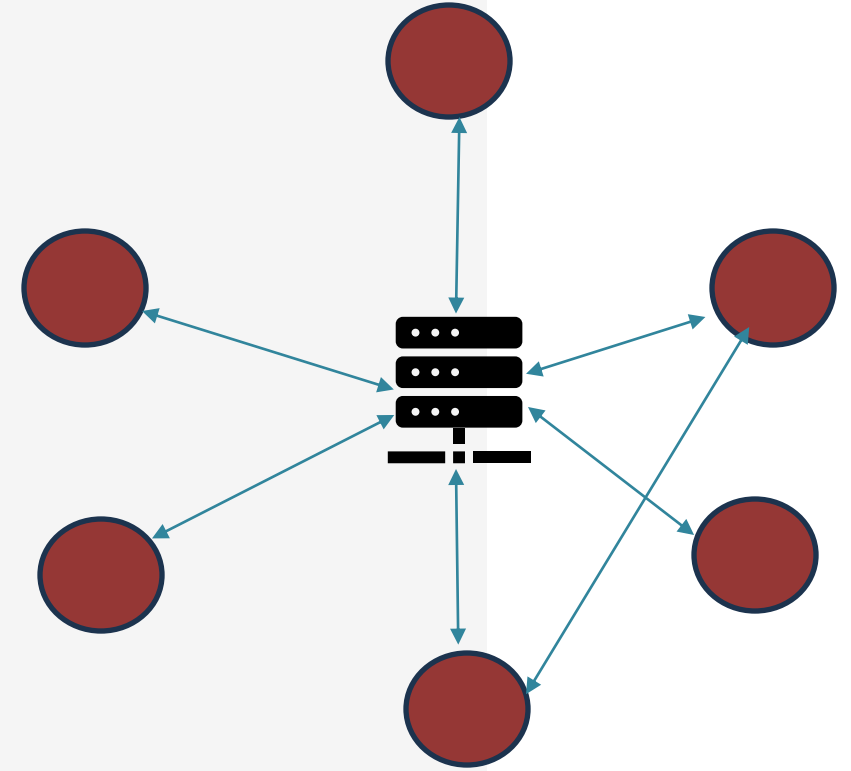
Again, What is a blockchain?

- To Summarize,
- Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cybersecurity concerns as a whole.
- Attractive properties of Blockchain
 - Log of data with digital signature
 - Immutable (once written - cryptographically hard to remove from the log)
 - Cryptographically secure - privacy preserving
 - Provides a basis for trusted computing on top of which applications can be built

Centralization vs Decentralization



- A decentralized peer-to-peer network
- Nodes are free to join and leave
- No central authority to create or impose rules



- A centralized network
- Nodes cannot join or leave without central authority's permission
- Central authority makes all the rules in the network
- There might be peer-to-peer connections but monitored by the central authority

Centralization vs Decentralization

- In a centralized system,
 - The data is stored in one location by a central trusted authority
 - Maybe one or two backup
- Issues
 - Vulnerable, under an attack all the data can be lost
 - Trust the central authority to not tamper the data
- Advantages
 - Easy to manage
 - Easy to provision--> easy to add or remove records
 - Easy to stop malicious activities

Centralization vs Decentralization

- In a decentralized system,
- Issues
 - Harder to manage
 - Harder to add or remove users
 - Harder to stop malicious activities
- Advantages
 - Replicated so robust against attacks
 - Democratic-->No unilateral decisions
 - Egalitarian --> All nodes are equal
 - Users can leave or join freely

Hybrid system

- Decentralization may be mixed with partial decentralization
 - Email
 - Decentralized protocol but dominated by few centralized webmail services

Decentralization in Blockchain

1. Who maintains the ledger?
 2. Who has authority over which transactions are valid?
 3. Who creates new blockchains?
 4. Who determines how the rules of the system change?
 5. How do bitcoins acquire value?
- The answer is not the same for all blockchains.
 - The central idea is same.
 - But different blockchain uses different variation of these ideas
 - Beyond the protocol
 - Exchanges
 - Wallet software
 - Service providers, etc.

Key takeaways

- The evolution of payment system
- Pros and cons of decentralized finance (DeFi)
- Challenges and solutions for DeFi
- Advantages and disadvantages of decentralization
- Bitcoin : Advantages and disadvantages
- Blockchain : Fundamental components and definition

Acknowledgement

- Much material in this course owe their ideas and existence to
 - Prof. Maurice Herlihy, Brown University
 - Prof. Hagit Attiya, Hebrew University
 - Prof. Arvind Narayanan, Princeton University
 - Prof. Joseph Bonneau, NYU
 - Prof. Pramod Subramanyan, IITK
 - Prof. Sandeep Shukla, IITK

The End !