Introduction to Blockchain and Traditional Finance (Trad-Fi)

Leon Godtfriedsen* Sahand Sarbaz† Josh Davidson‡
Jose Garrido Boix§

September 2025

*Lead author, University of Edinburgh
†Co-author, University of Edinburgh
‡Co-author, University of Edinburgh
§Co-author, University of Edinburgh

Week 1 - introducing blockchain/crypto-currencies, history of money and traditional finance (trad-fi) systems.

Introduction to, and Background of, Blockchain:

There have been countless forms of digital money, many of which have failed. The failure was due to lack of cryptographic capabilities. The dawn of the internet, and with it cryptography, paved the way for digital currencies.

History of internet:

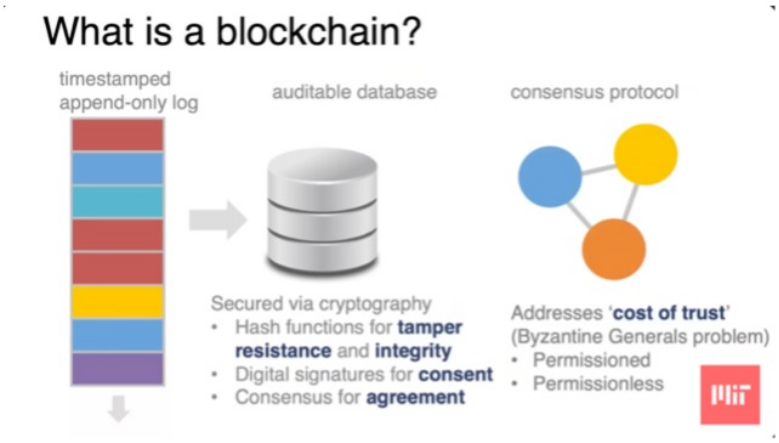
- Ethernet: 1974
- TCP/IP: 1974
  - Network research and file transfer.
- HTTP: 1990
  - Allowed for creation of world wide web – interactional, yet insecure sites.
- SSL/TLS: 1996 – Asymmetric crypto stack layered on top of http.
  - Dawn of new internet age: Pay online, Gmail etc.

  Development of cryptography is what enabled the development of internet and subsequently paved the way for digital currencies. However, forms of "digital currencies" have existed prior, for example:

- MPESA: Unbanked people in Kenya trading data minutes as a form of currency.
  - Half of Kenya was unbanked – but they all had cell phones – and started trading cell phone minutes.

  This cryptographic development allowed for Blockchain:

  - Blockchain was founded long before bitcoin – first was in the 90's
  - Consists of: Time stamped append only log + onto an auditable database + secured via cryptography



Potential Opportunities for blockchain in financial sector:

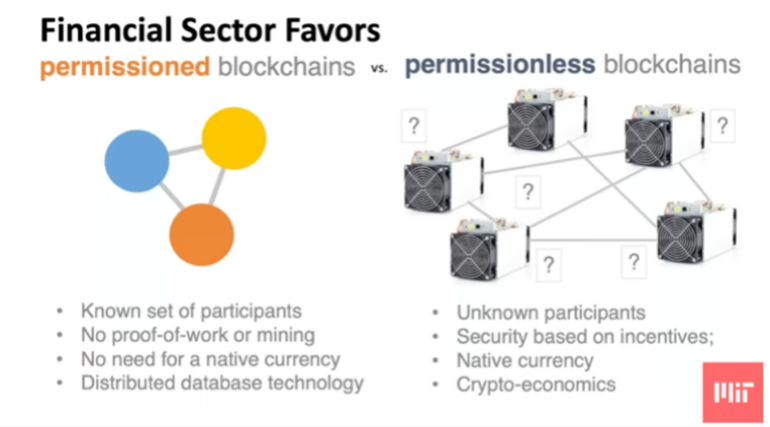
- Fiat currency insecurity associated with unsound policies: Reduction in reliance on poor monetary policy/governments
- Centralised intermediaries concentrate risk
- Central Bank Legacy Payment System: Still pay 2.5-3% fee
- Financial Inclusion
  - 1.7 Billion people are unbanked: Payment system is 0.5% of US economy

Potential Issues for Blockchain in financial sector:

- Performance, Scalability, Efficiency: BTC only does about 7 transactions per second (txps), visa can do about 100,000txps
- Privacy and Security: Blockchains are public financial services require a level of privacy, blockchains breach GDPR and similar regulations $\rightarrow$ Creation of censorship resistance is making public services worry as they have no ability to control movement of funds or reversal of transactions.
- Interoperability – ability of different blockchains to communicate and carry out transactions.
- Governance

  - Decentralised therefore no-one can "update" etc.

- Commercial Use Cases
  - Haven't been entirely discovered yet.



Public Policy Frame Work: What is the governments focus with CC's?

- Guarding against illicit activity
  - People say it will only be used for crime. Crime has always been present, mechanisms and means will change. Proportionally similar amounts are used for illicit activities in Traditional-Finance vs Decentralised-Finance
- Financial Stability
  - People can use to avoid capital controls
  - However, crypto is $3T, finance is $400T so minor effect in grand scheme, as of yet. Blockchain forensics also changes this landscape.
- Protecting the investing public

In essence: blockchain provided P2P transactions whilst removing cost of trust.

- Financial sector and Fiat Currencies have had challenges

  - Run on banks, inflation, poor monetary policy provides case for decentralised system

- Money is just a social & economic consensus, BTC can be too

History of Money

Money: Social Construct / Consensus Mechanism

BTC has no inherent value → Value comes from social construct → However not backed by central authority (maybe the value of modern cash attributed to inter/national backing)

- Some argue the processing power behind BTC is the source of value/backing.

The beginning of the financial system started with ledgers.

- Funnily enough, Blockchain is based on a more "complicated" ledger.

Ledgers and double entry book keeping → Started financial society → BTC is natural extension

- A Store Clerk would, with double entry book keeping, note their trades
- Progressed to bankers/merchants storing value on behalf of customers
  - This progressed to "cash", with guarantees by merchants (rest is history)

Quick overview of the History of money:

- First salt was used in Ethiopia, due to its practical value:
  - This was taken advantage of during slave trade
- Then Rai Stones: large stone discs, scarce initially which is a plus but difficult to transport and therefore exchange.
  - Taken advantage of by British explorers who created falsified Rai stones, leading to currency devaluation and eventually hyperinflation
- Then Metal money:
  - Intrinsic value of the coins as well a durable and easy to transport– however quickly became impractical due to difficulty of determining purity for every transaction.

- Then stamped metal money:
  - Central Authority standardised purity, weight and size of coins, ensuring currency was trustworthy.
- Then came Paper Money:
  - Started in China 700BC where trusted parties would hold copper currency in exchange for paper receipts, was essentially unofficial warehouse ledgers. Chinese government soon got involved and created first official paper currency. Eventually gold smiths (secure vaults) became bankers with gold standard backing value of the currency they handed out.

Point to note is that forms of money throughout history have been designed to be less susceptible to manipulation and exploitation. Would BTC/other CC's be a natural step forwards from where we are now?

Money needs to have these traits:

- Medium of exchange
- Store of Value
- Unit of account

Does BTC have these qualities? Does gold?

Ledgers and the Traditional Financial System

Ledger: Way to record economic activity and/or financial relationships (DEBT)

Types of Ledgers: Transaction Ledger (BTC) Vs. Balance Ledger (ETH) General Ledger (Overall picture) Vs. Sub-Ledger (specifics) Central Bank is General Ledger for money. The regional banks keep the specific accounts

Single Entry Ledger, Double Entry Book Keeping: A debit to one account, and credit to another account → Difference is capital → Started Capital Markets

Financial System is BASED on ledgers. Characteristics of good ledger:

- Immutable
- Time Stamped
- Ownership

- Accuracy
- Description of transaction

Ledgers and money overlap significantly. BTC is essentially a cryptographic, decentralised ledger, hence its use case as a "currency". Why this introduction to ledgers now?

Traditional Payment systems are essentially a way to amend ledgers.

Fiat Currency:

Fiat Currency is fundamentally built on these blocks:

- Social and Economic Consensus (based off government backing)
- Represents liabilities of central banks
- Central Bank (General Ledger), with regional banks (sub-ledgers)

Deposit in a bank is a liability for a bank. They were initially liable for gold, but now liable for a person to move their deposit to another bank. Move ledger.

General Function of Banking System:

Starts with: transactions between different individuals at different banks. → Commercial Bank Communicates with each other and exchanges information on different ledgers. They move the persons balance from one ledger to the other banks ledger. → Commercial banks communicate with federal bank to update the general ledger. →

- The US has been on and off the gold standard the past 140 years. Its value is solely derived from social consensus.
- The US$ has these traits:
  - Medium of exchange
  - Store of Value
  - Unit of account
- The banking system provides the ledger for the US$ to operate having:
  - Immutable

  - Time Stamped
  - Ownership
  - Accuracy
  - Description of transaction

But why did early digital currencies fail?

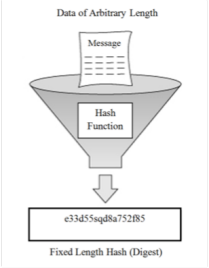
- Merchant adoption
  - Technology was too novel, and there was a lack of technological know-how for it to become prominent.
- Centralisation
  - Previously controlled by very few nodes which acted as large points of failure/vulnerability.
- Double spending: BTC solved this
  - Double spending is the idea that the same digital currency can be spent twice in different tx's. Bitcoin solved this by using a decentralized, proof-of-work blockchain where every transaction is time-stamped, publicly verified, and added to an immutable ledger, preventing the same coin being used twice.
- Consensus: The issue of getting many nodes to gain consensus (POW)

Quick Introduction to BTC

BTC as mentioned is essentially: Cryptography + Consensus Algorithm + Ledger

Cryptographically we have:

- Hash Functions
  - A hash function is a one-way mathematical algorithm that converts any input into a fixed-length output, and in Bitcoin it's used to secure transactions, link blocks together, and enable Proof-of-Work mining by requiring miners to find a hash below a target value.



- Private, Public Key's & Digital Signatures
  (asymmetric cryptography):
  - A private key is a secret used to sign transactions, while the corresponding public key allows anyone to verify ownership and authenticity without revealing the secret.
- Block heads and Merkle Tree Structure
  (way to compress data)
  - A block header stores metadata (hash of previous block, timestamp, nonce, Merkle root, etc.), while a Merkle tree efficiently summarizes and verifies all transactions in the block by hashing them into a single root included in the header.
- Nonce's
  - The nonce is just a number that miners keep changing until the block's hash starts with enough zeros to meet the difficulty rule, like guessing different combinations until one unlocks the block

Consensus Algorithm: The way to get all nodes supporting the network to come to agreement

- Light and Full Nodes (Nodes validate transactions (tx), full nodes store entire tx list)
- Solves Byzantine Fault Problem
  - The Byzantine fault problem describes the challenge of achieving agreement in a distributed system where some participants may fail, lie, or act maliciously, making it difficult to know which information is trustworthy.
- Proof of Work (BTC's actual consensus algorithm):
  - Where miners compete to add blocks, and the longest valid chain is accepted by the network—making it computationally infeasible for dishonest actors to override the majority.
- Native Currency
  - Incentive Mechanism for Nodes

Ledger:

- Time stamped append only logs
- Also functions with Unspent Transaction Output (UTXO) systems but this will be discussed in more detail later

This introduction to BTC provides the necessary backdrop to teach the remaining and more complicated cryptographic features of BTC.