Introduction to Blockchain Technologies

Ioan Raicu
Computer Science Department
Illinois Institute of Technology

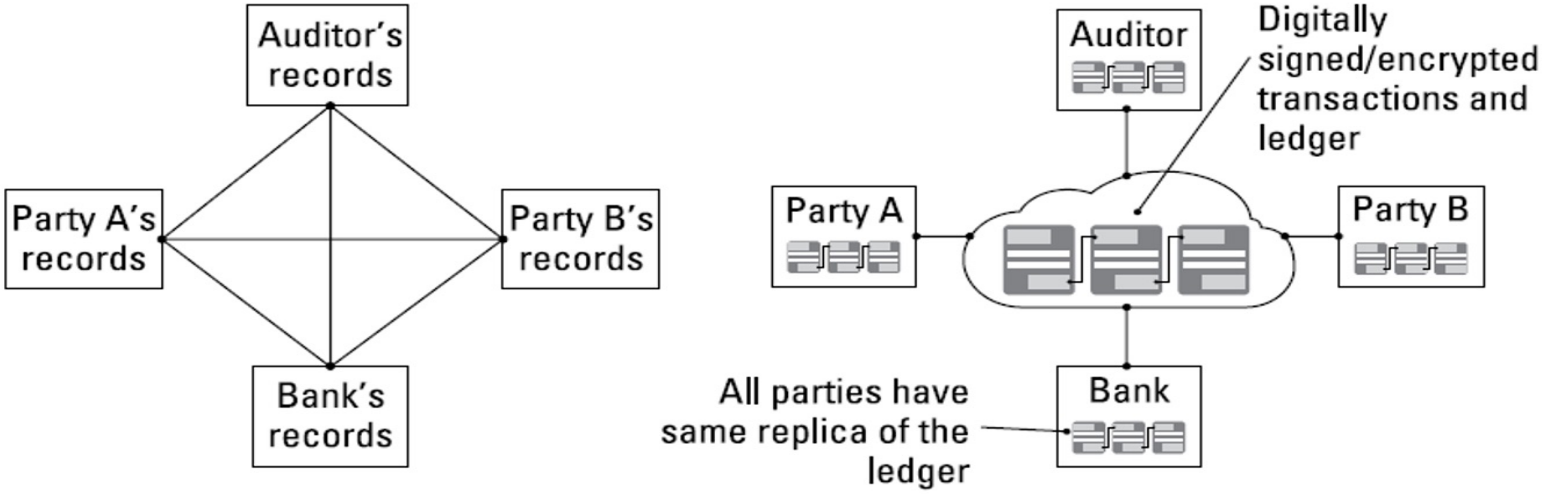
CS554: Data-Intensive Computing
January 24th, 2023

Reading Material

- Distributed Systems (no writeup needed)
  - Maarten van Steen, Andrew S. Tanenbaum. A brief introduction to distributed systems.
  - Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. "*Cloud Computing and Grid Computing 360-Degree Compared*", IEEE Grid Computing Environments (GCE08) 2008, co-located with IEEE/ACM Supercomputing 2008.
- Blockchain Technologies (HW1 posted, due Wed 01/25)
  - Wikipedia Article on Blockchain: https://en.wikipedia.org/wiki/Blockchain
  - Wikipedia Article on Satoshi Nakamoto: https://en.wikipedia.org/wiki/Satoshi_Nakamoto
  - Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

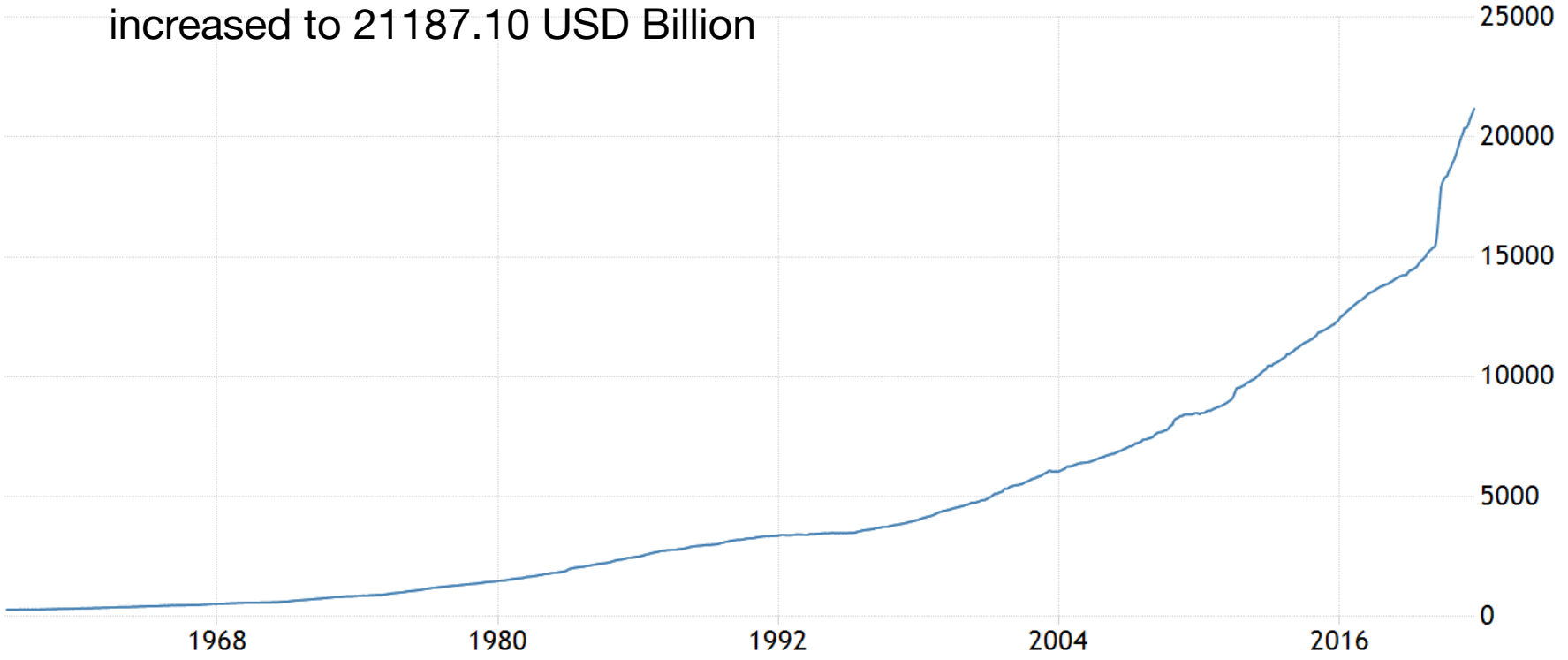
Tracing Blockchain's Origin

- **The shortcomings of current transaction systems**
  - **During 2000's financial crisis**



Inflation

Money Supply M2 in the United States increased to 21187.10 USD Billion



SOURCE: TRADINGECONOMICS.COM | FEDERAL RESERVE

Bitcoin Whitepaper: 10/31/2008

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

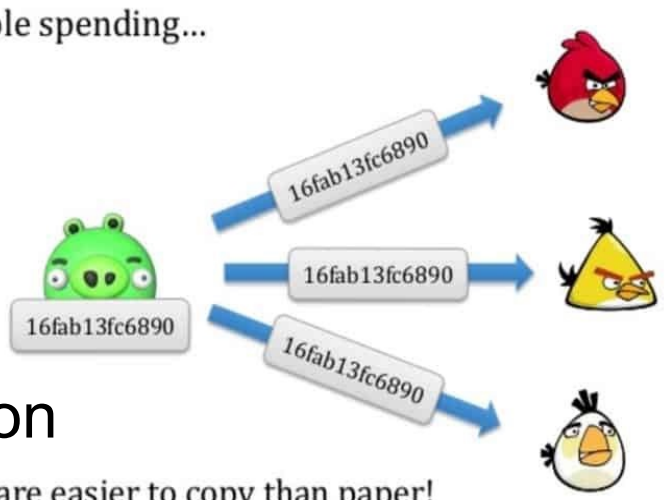
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Digital Currency

- The most successful among lot of efforts: Bitcoin
- Replace cash with numbers and codes
- Advantages
  - Fast
  - International
  - Easy accounting
  - Weighs nothing
  - Cheap
- Problems to be solved

Problems of Digital Currency

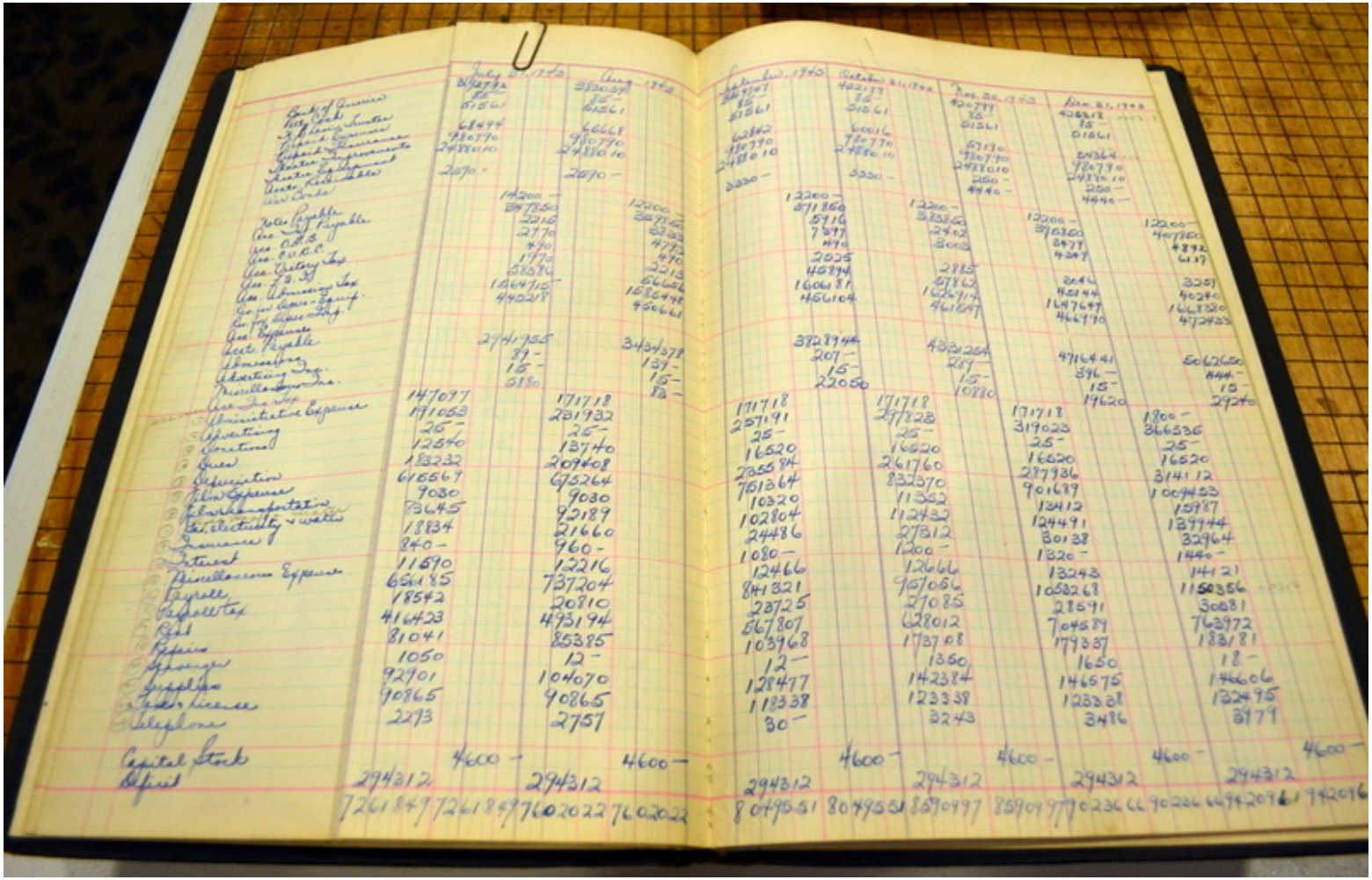
- Perfect Copy
  - Just like downloading attachment from email
  - How to distinguish counterfeits
  - Ownership Problem
- Double Spending
  - Networks are noisy and transmission across networks is far from instantaneous: delay
  - A hacker can capitalize
  - Fraudster Detection Problem



The Long Road to Bitcoin

- Centralized Banking: not robust
- Satoshi determined to find the centralized part of banks
  - The ledger
  - “What if I could turn a bank inside out? Instead of one central party controlling the ledger, what if every user were recruited to maintain a constantly updated copy?”
- The strength of the digital was perfect copies, so copy the ledger, everywhere, instantly.
  - Any ledgers with even one common not agreeing with the masses would be discarded, leaving fraudsters powerless
- **Replace cash with Ledger!**

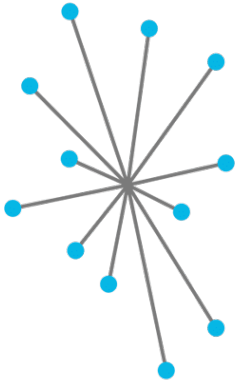
Ledger



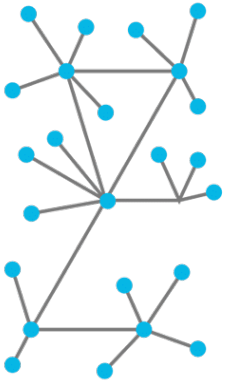
Decentralization

- Replace cash with Ledger

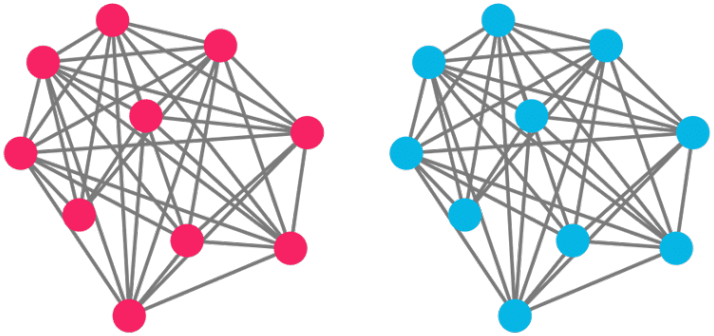
Centralized



Decentralized



Distributed Ledgers



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

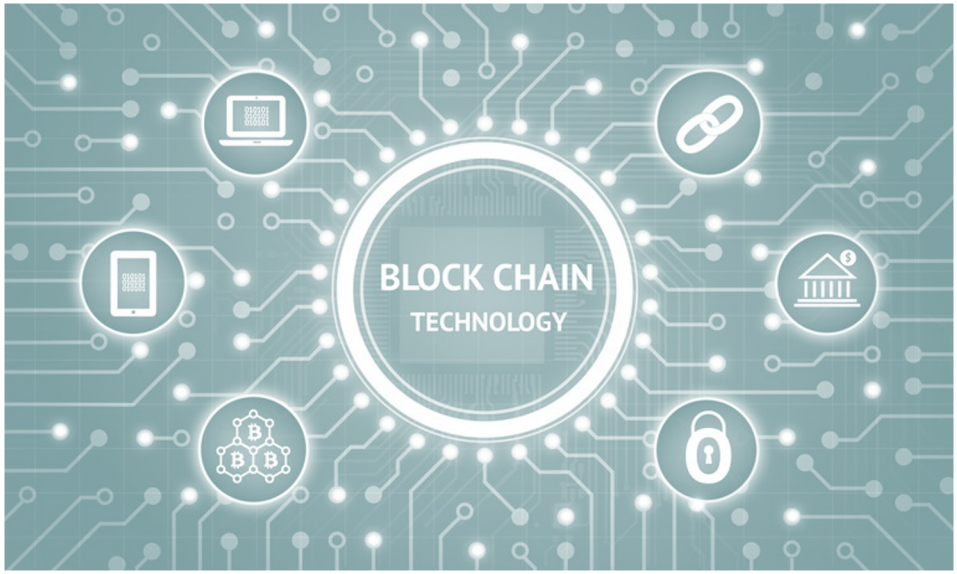
Blockgeeks

The decentralized ledger (Blockchain)

- Decentralization: get rid of the Third Party
- Satoshi paired two main technologies
  - Proof of Work: to solve the double spending problem & leader election
  - Elliptic Curves: to solve unique access to the ledger
- Nothing was newer than 2001
  1. 2001: SHA-256 finalized
  2. 1999-present: Byzantine fault tolerance
  3. 1999-present: P2P networks
  4. 1998: Wei Dai, B-money
  5. 1998: Nick Szabo, Bit Gold
  6. 1997: HashCash
  7. 1992-1993: Proof-of-work for spam
  8. 1991: cryptographic timestamp
  9. 1980: public key crypto algorithm

What is Blockchain Technology

- Bitcoin stores all its transactions onto a public database called as Blockchain

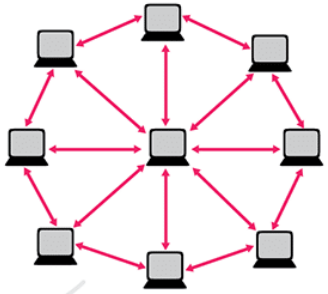


Upcoming Seminars

- 02/02/23 SB111@12:45pm
  - Designing Exascale Distributed Systems
  - Extra Credit: Attend, ask a question, write a 250-word summary of the talk, due 2/2/23 at 11:59pm on BB
- 02/09/23 SB233@12:45pm
  - Context-aware Responsible Data Science
- 02/10/23 Zoom@12:45pm
  - Text Simplification: Methods and Evaluation

Highlights

Someone requests a transaction.



The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger,**

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

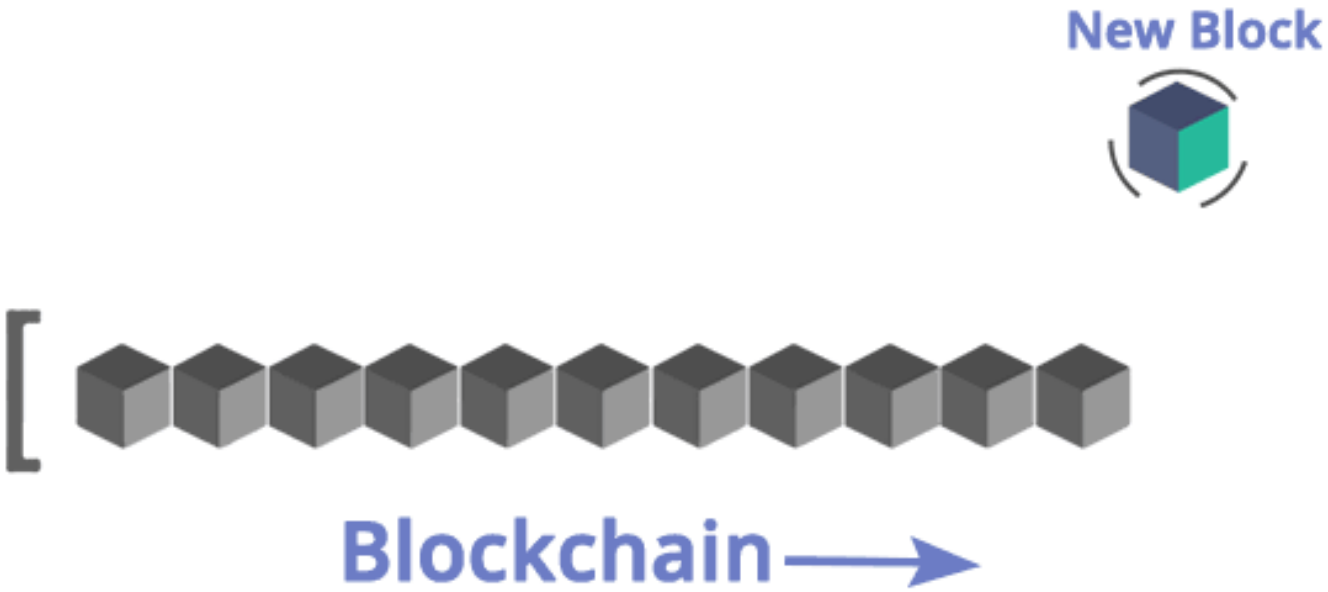
cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Has no physical form and exists only in the network.

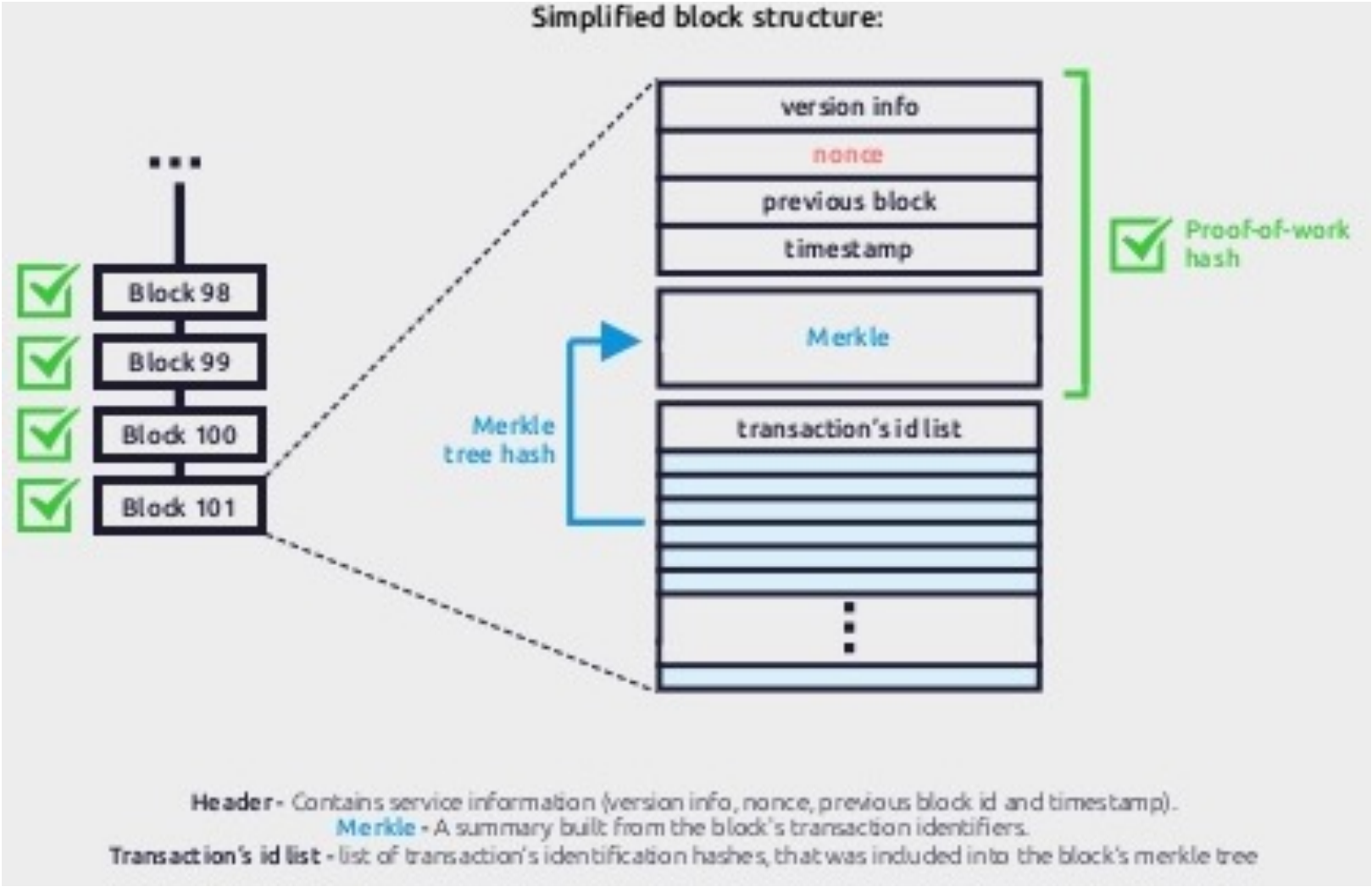
Its supply is not determined by a central bank and the network is completely decentralized.

Blockchain Structure



Source: https://www.edureka.co/blog/blockchain-tutorial/

What does a block look like?



Upcoming Seminars

- 02/07/23 SB111@12:45pm
  - Real-time DNN Execution on Mobile Devices with Compiler Optimizations
  - Extra Credit: Attend, ask a question, write a 250-word summary of the talk, due 2/7/23 at 11:59pm on BB
- 02/09/23 SB233@12:45pm
  - Context-aware Responsible Data Science
- 02/10/23 Zoom@12:45pm
  - Text Simplification: Methods and Evaluation

4 Key Concepts of Blockchain

Distributed shared ledger

Cryptography

Consensus

Smart contracts

Source: IBM, A new disruption in financial services

Blockchain: Distributed Ledger Technology

Defining Blockchain

A distributed ledger technology

Blockchain is a cryptographic, or encoded ledger – a database of transactions in the form of blocks arranged in a chain. These are validated by multiple users through consensus mechanisms (such as proof-of-work in Bitcoin mining) shared across a public or private network.

Blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance

Potential benefits of Blockchain technology for the financial services industry

- Reduce costs of overall transactions and IT infrastructure
- Irrevocable and tamper-resistant transactions
- Reduction in systemic risks (eliminate credit and liquidity risks)
- Consensus in a variety of transactions
- Ability to store and define ownership of any tangible or intangible asset
- Increased accuracy of trade data and reduced settlement risk
- Near-instantaneous clearing and settlement
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators

2009-2012 Foundation days

- Emergence of Bitcoin based on a paper by Satoshi Nakamoto
- On January 3, 2009, the Genesis block was mined
- Experimental and limited to cryptographic community
- Blockchain as the backbone of Bitcoin

2012-2014 Moving beyond the cryptographers

- Rise of Bitcoin exchanges
- Mixed response to Bitcoin as it struggles with money laundering and criminal activity, but also gains acceptance across some online retail stores among others
- Rise of Bitcoin- based startups
- Bitcoin price surged to US$1,000
- Blockchain gains attention of financial services firms (begins internal trials)

2014-2015 Blockchain buzz years

- Blockchain, the underlying technology behind Bitcoin, gets serious attention and investment from financial services firms, regulators, and VCs
- Explosion of use cases within BFSI
- Announcement of consortiums to accelerate adoption, innovation, and common standards
- Banks experiment with their versions of cryptocurrencies
- Global service providers and technology companies put their weight behind Blockchain

2016-2017 Crossing the chasm

- The next two years are critical for Blockchain technology to demonstrate sustainable value and show adoption beyond proofs of concept by FS firms
- Startups backed by VC funding and consortiums need to show results to justify the large sums of funding and/or investment of time and resources
- Scalability and throughput issues need to be solved for the Blockchain technology to cross the chasm to mainstream adoption

2018-2020 Adoption movement

- Consortiums will be instrumental in defining protocols and common standards to facilitate widespread adoption
- Regulatory bodies likely to play a key role in facilitating adoption while ensuring compliance
- Explosion of use cases beyond BFSI
- IT service providers likely to accelerate investments to build capabilities around Blockchain technology implementation
- Rise of IPOs and Unicorns in the Blockchain startup ecosystem

2020 & beyond Accelerated adoption

- Blockchain will gain adoption within and beyond BFSI, leading to new business models at the intersection of advanced analytics, IoT, and Blockchain based smart contracts
- Blockchain is referenced in two major shifts expected to occur in the nearest future, according to a report by World Economic Forum: The first tax collected by government using the Blockchain technology by 2023. The second one is storing more than 10% of global gross domestic product in Blockchains by 2027
- Banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance reduced by US$15-20 billion a year from 2022, according to a recent report by Spanish bank Santander

Bitcoin System vs. Current Banking System

- **Decentralized System**
  - The Blockchain system follows a decentralized approach when compared to banks and financial organizations which are controlled and governed by Central or Federal Authorities.
  - Here, everyone who is involved with the system holds some power.
- **Public Ledgers**
  - The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system.
  - Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous.
- **Verification of Every Individual Transaction**
  - Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes.
  - Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated.
- **Low or No Transaction Fees**
  - These transaction fees are however relatively quite less when compared to the fees implied by banks and other financial organizations.
  - If a transaction needs to be completed on priority then an additional transaction fees can be added by the user so as to have the transaction verified on priority.

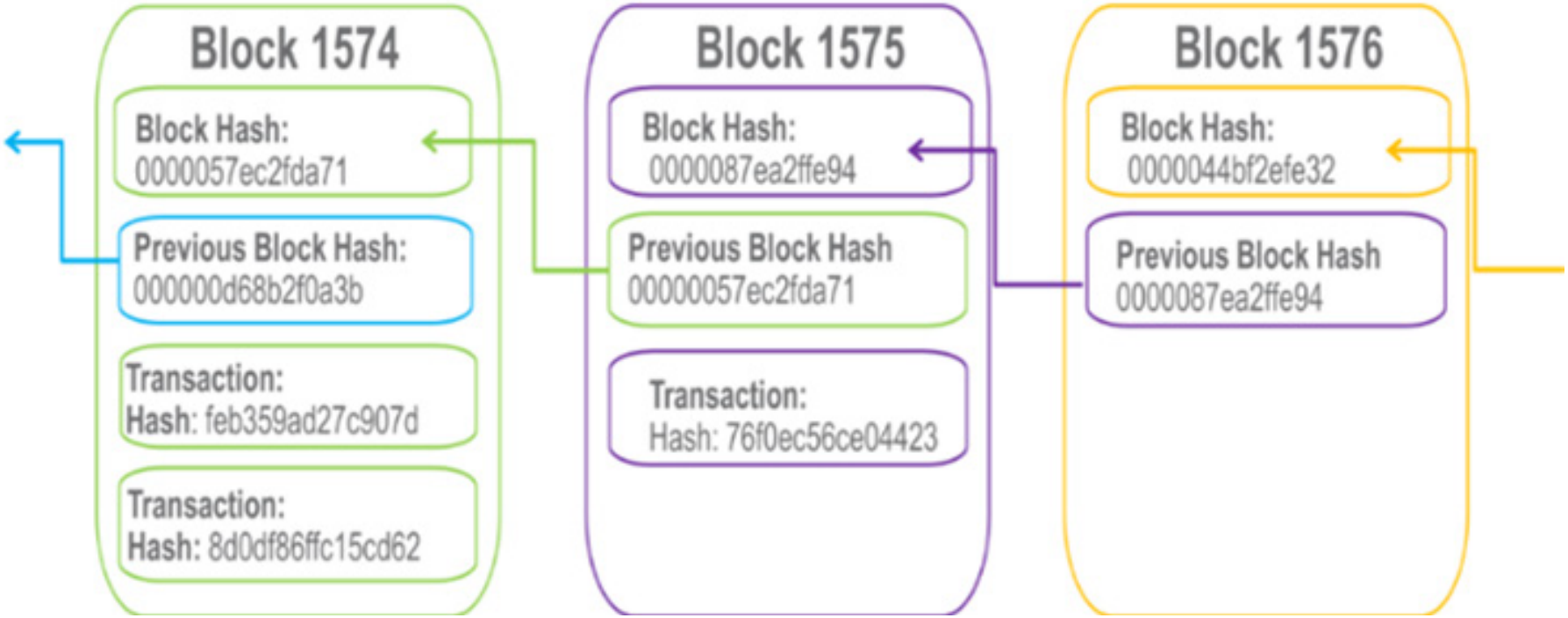
the key business benefits

- **Time savings:**
- **Cost savings:**
- **Tighter security:**
- **Enhanced privacy:**
- **Improved auditability:**
- **Increased operational efficiency:**

Building trust with blockchain

- **Distributed and sustainable:**
- **Secure, private, and indelible:**
- **Transparent and auditable:**
- **Consensus-based and transactional:**
- **Orchestrated and flexible:**

Why It's Called "Blockchain"



How is Blockchain kept secure?

- Proof of Work
- Proof of Stake
- Proof of Space
- Proof of Time
- Pros and cons?

Top 10 Coins in 2023

- Bitcoin
- Ethereum
- Tether
- USD Coin
- Binance
- XRP
- Binance USD
- Cardano
- Dogecoin
- SOL

Other Notable Coins

- MATIC
- DOT
- Bitcoin Cash
- Litecoin
- Chainlink
- Ethereum Classic
- Shiba Inu
- XCH
- Luna

Major Exchanges in the US

- Binance
- FTX
- Coinbase

Questions