Distributed Ledger Technology and Censorship Resistance

Armin Krishnan

East Carolina University

The future is decentralized.

Or: the future is peer-to-peer sharing.

Outline

1. Argument
2. What Is Blockchain Technology?
3. Financial Applications of Blockchain Technology
4. Smart Contracts and Other Applications
5. Decentralized Storage
6. What Makes Blockchains More Secure?
7. Why Censorship Resistance Matters
8. What Makes Blockchains Censorship Resistant?
9. Censorship Resistant Websites
10. Decentralized WikiLeaks
11. Conclusions

1. Argument

- Blockchain or Distributed Ledger Technology will make data storage more decentralized, more secure, and more resistant to censorship. This will have both positive and negative implications for governments and other centralized organizations, including traditional libraries.

2. What Is Blockchain Technology?

- The blockchain was invented by Satoshi Nakamoto in 2008 and explained in the White Paper “Bitcoin: A Peer-to-Peer Electronic Cash System” published on the Internet.
- Bitcoin was a response to the 2008 Financial crisis and it likely came out of the cypherpunk movement - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.“ Block 0 (Genisis Block)
- From around 2010 there have been a number of other blockchain projects that compete with Bitcoin – some of the early projects that are still active are Litecoin LTC, Ripple XRP, and Dogecoin Doge.
- In July the smarts contracts platform Ethereum was launched by Vitalik Buterin, which has added programmability to blockchain technology – it is called **Blockchain 2.0**.
- From 2018 projects have been launched to address scalability and blockchain interoperability issues, which is referred to as **Blockchain 3.0**.

2. What Is Blockchain Technology?

The Cryptocurrency Market (April 2021)

- Coinmarketcap lists over 9400 ‘coins’ or projects that sell digital tokens
- The overall market valuation is greater than $2 trillion (the gold market has valuation of $3.7 trillion)
- Bitcoin has a price of $56,000 per unit with 18.6 million units in circulation
- It costs $3,000-$4,000 to mine a Bitcoin, which makes Bitcoin mining immensely profitable at this time
- Major banks, investment funds, and universities have invested in cryptocurrencies
- Distributed Ledger Technology (DTL) is going mainstream and is considered a disruptive technology as it will change the way businesses and society operates

2. What Is Blockchain Technology?

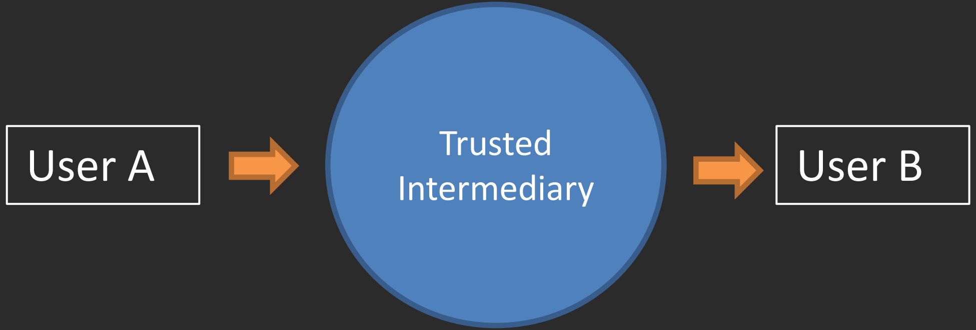
- Vitalik Buterin: “Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.”
- Amir Taaki: “Bitcoins aren’t a f… payment innovation… Bitcoins are a political project.”
- Naval Ravikant: “Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme.”

2. What Is Blockchain Technology?

- “Peer-to-Peer version of electronic cash”
- Distributed ledger that records and confirms transactions with consensus protocol
- Public-key encryption (256 bit) is used to sign transactions on the blockchain – every transaction is protected by a unique cryptographic hash
- ‘Proof-of-work’ algorithm makes transactions irreversible and creates an immutable record of transactions that is distributed over a large number of nodes

2. What Is Blockchain Technology?

Traditional Transactions



User A → Trusted Intermediary → User B

Single point of failure

2. What Is Blockchain Technology?

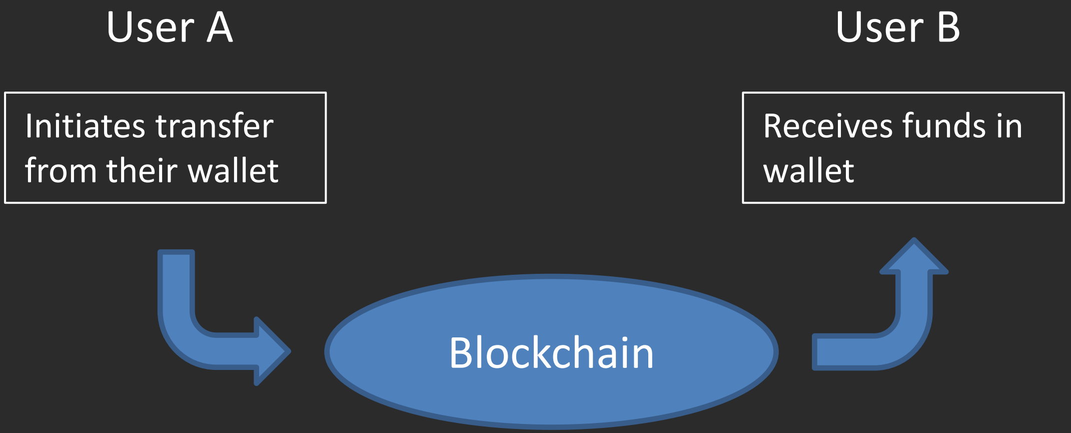
- A cryptocurrency wallet consists of a public key or address, e.g.:

  bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

- The wallet is controlled with a private key – it is not possible to recover the private key from the public key.
- Each transaction is signed with a hash of the private key that authorizes it – it is not possible to recover the private key from the signature hash.

  92bf49e0a52b0cc06a6793943b885390aada26558740c382dba9937c5d2caace

2. What Is Blockchain Technology?



User A

Initiates transfer from their wallet

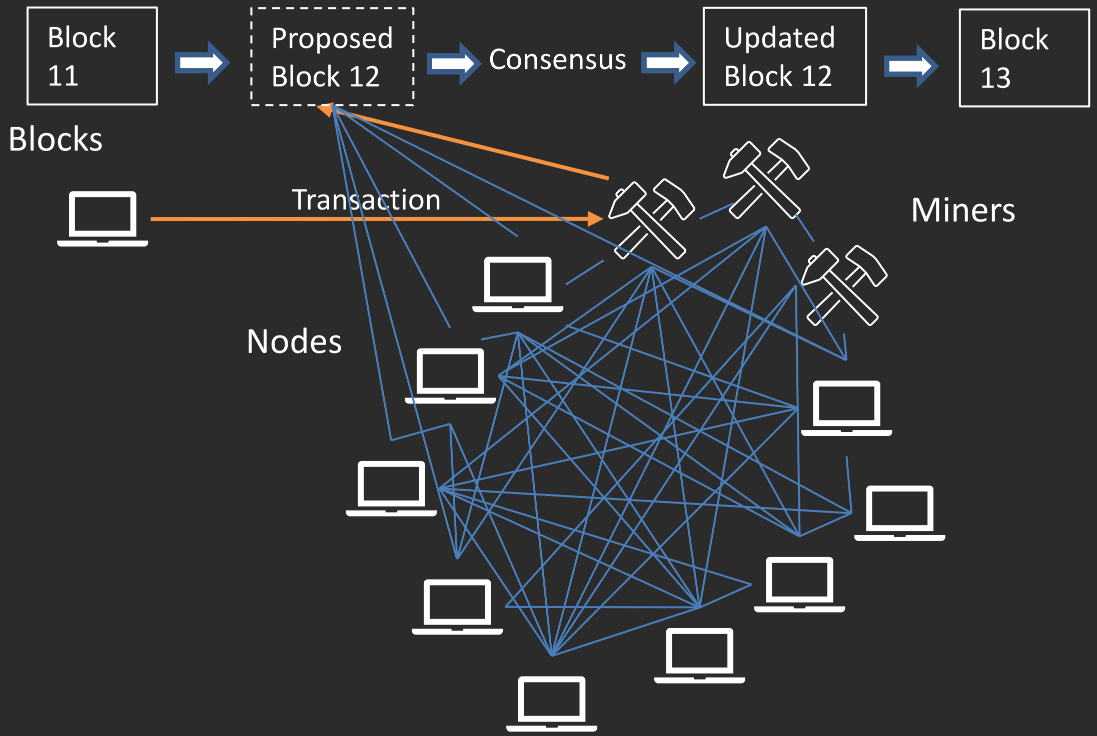
Blockchain

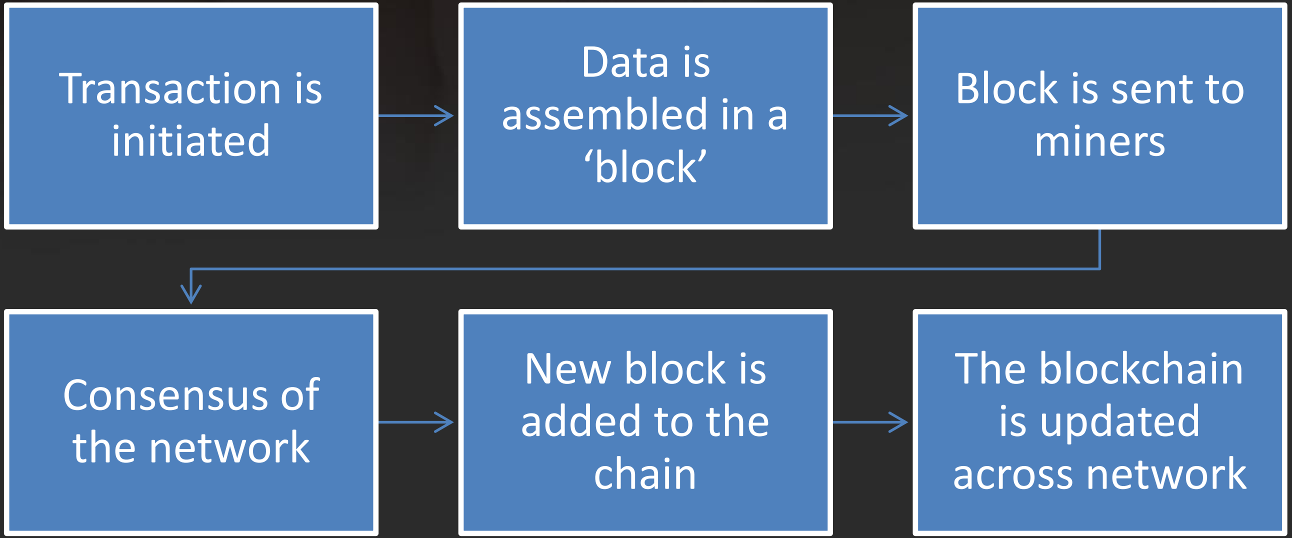
User B

Receives funds in wallet

Peer-to-peer transactions

2. What Is Blockchain Technology?





Transaction is initiated

Data is assembled in a ‘block’

Block is sent to miners

Consensus of the network

New block is added to the chain

The blockchain is updated across network

2. What Is Blockchain Technology?

- Anybody can 'mine' Bitcoin by connecting a computer to the network and running the Bitcoin protocol
- The miners solve a cryptographic puzzle and the first to solve it gets the block reward of 6.25 Bitcoin (2020 halving)
- Trust is distributed across the network: as long as a majority of nodes does not participate in an attack a fraudulent transaction will not be confirmed.
- There are 10,000 Bitcoin nodes distributed over a hundred countries in the world.

2. What Is Blockchain Technology?

Blockchain and the Currency Aspect

- Some commentators have misleadingly suggested that blockchain will succeed as a transformative technology, but not decentralized cryptocurrency.
- It makes no sense to separate blockchain and the currency component since doing so would take away most benefits of having decentralized system.
- There have to be block producers or miners who need to be compensated for the work that they do – the best way of doing so is to pay them in tokens that reside on the blockchain.
- Otherwise there would need to be a centralized entity that runs all miners, which creates a single point of failure and requires the whole network to trust that entity.

3. Financial Applications of Blockchain Technology

- Bitcoin has solved the ‘double-spend’ problem of decentralized digital cash.
- It functions as a currency that can be sent peer-to-peer with no need for a trusted third party.
- Owners of Bitcoin control the record on the blockchain associated with their public key or wallet address through a private key consisting of 64 alphanumeric characters (256 bit encryption).
- Crypto assets cannot be frozen, transactions cannot be reversed by a central authority, and they are hard to confiscate as this requires access to a private key.

3. Financial Applications of Blockchain Technology

- Money laundering and criminal use of digital currencies has been a concern for decades.
- Bitcoin was the means of payment on the Silk Road illicit marketplace.
- There is anecdotal evidence that terror groups and criminal organizations have used digital currencies, but not in a systematic way.
- In principle, every Bitcoin transaction is visible on the blockchain and can be tracked – Bitcoin owners may be unmasked with special methods of analysis and computer forensics.

3. Financial Applications of Blockchain Technology

- Privacy coins like DASH, Monero, and ZCASH use coin-mixing, zero-knowledge proof protocols, and the encryption of transaction values to make it hard to track transactions on the blockchain.

3. Financial Applications of Blockchain Technology

Decentralized Finance (DeFi)

- Stable coins
- Decentralized lending (use of crypto as collateral)
- Decentralized exchanges (DEXes)
- ‘Wrapped’ Bitcoin
- Prediction markets
- Yield farming

4. Smart Contracts and Other Applications

- Ethereum
- ‘Smart Contracts’
- Trustless transactions
- Tokenization
- Internet of Things

4. Smart Contracts and Other Applications

- Bitcoin operates like a DAO
- ‘The DAO’ (2016)
- Crowd-sourcing initiative for Ethereum-based projects
- Sale of tokens and voting by the community on the blockchain
- ‘The DAO’ failed but the concept is sound

4. Smart Contracts and Other Applications

- Supply chain and logistics management
- Blockchain voting
- Personal identity security
- Non-fungible tokens (NFTs)
- Internet of Things (IoT)
- Decentralized data storage
- Decentralized computing
- Decentralized social media
- Decentralized publishing

5. Decentralized Storage

- Data can be stored on any computer (miners) connected to the Internet that makes resources available in exchange for block rewards (native tokens).
- The price for storage is decentrally controlled by the market (supply and demand for storage).
- Clients can enter into ‘smart contract’ with miners that specifies the duration and price for stored data.
- Files are stored through the Interplanetary File System protocol.
- This approach optimizes computing resources and connects suppliers of storage with users of storage.

5. Decentralized Storage

The Interplanetary File System (IPFS):

- Developed in 2015, IPFS is a protocol for a peer-to-peer network for data-sharing
- Files can be retrieved by their content address from any node that holds it
- Since the IPFS works peer-to-peer it is impossible to block this content on the Internet

6. What Makes Blockchains More Secure?

- Blockchains are based on strong cryptography and cryptographic protocols.
- It has been suggested that there are more possible private Bitcoin addresses than there atoms in the world – it is currently impossible to access Bitcoin by guessing a private address (quantum computing might change this, but it is still far off).
- Every transaction has to be authenticated and must confirmed by a network consensus before it is permanently recorded on the blockchain.

6. What Makes Blockchains More Secure?

- Although data is stored on public blockchains any alteration of the data is protected by encryption.
- Sensitive information on blockchains can be encrypted, e.g. encrypted blockchain databases.
- There is no single point of failure as in the case of cloud storage.
- Private transactions are possible on blockchains.

7. Why Censorship Resistance Matters

- More and more information only exists in digital form – hard copies are often no longer used.
- Digital information that is centrally stored in a cloud or in a central database can be easily altered or deleted, in which the original information is lost.
- **Problem:** how can a user know that the information is authentic and complete and has not been tampered with?
- **Example:** in 2009 Amazon secretly deleted digital copies of 1984 from Kindle devices (due to copyright issues) – in theory a centralized provider could distribute altered copies of 1984 or completely erase the book with users having no ability to check the authenticity (unless they have an original hard copy) or recover the text.

7. Why Censorship Resistance Matters

Internet Censorship

- Internet backbone filtering
- DNS interference
- Blocking of websites by ISPs
- DDOS attacks
- Removal of content by platforms
- Search engine manipulation
- Shadow banning
- Server takedown
- Self-censorship

7. Why Censorship Resistance Matters

- **Internet censorship by governments and corporations is a threat to society:**
  - Political dimension: infringes on freedom of speech and silences dissent; people can be made nonpersons
  - Knowledge dimension: destroys or alters knowledge according to political and economic imperatives, which can affect progress

8. What Makes Blockchains Censorship Resistant?

Immutability

- Transactions are irreversible: once a transaction is approved by network consensus there will be a permanent record of the transaction stored in the respective block.
- Each validated block is cryptographically signed with a hash – a hash is a one-way function that allows information to expressed in a hash without the possibility of recovering the original information from the hash.
- The blockchain is distributed across a larger network, meaning that every node has a complete copy of the entire blockchain with every transaction that has ever taken place on that blockchain.

8. What Makes Blockchains Censorship Resistant?

Central authorities cannot:

- Take down content that resides on a blockchain as there is no single entity that can alter the blockchain.
- The takedown of a blockchain stored in multiple jurisdiction would require global government cooperation, which is unlikely.
- Servers could be located off-shore or in space, which means outside of the jurisdiction of any government.

9. Censorship Resistant Websites

Unstoppable Domains

- Uses a Crypto Name Service (CNS) instead of a Domain Name Service (DNS).
- Uses smart contracts on a blockchain for the creation and management of domains.
- Once a new domain is created it is irrevocably owned by the creator – it cannot be taken down by a central authority – it might be simply delisted from search engines and would be difficult to find.

9. Censorship Resistant Websites

- Censorship-resistant websites are important for making it impossible for any single authority or group of entities to control all information available to the public.
- Since 2020 governments around the world have cracked down on digital content related to COVID that they did not agree with – the idea that any undesirable content can be labelled extremist or nonfactual and removed undermines transparency and accountability, which leads to political repression and bad science.

Decentralized WikiLeaks

- WikiLeaks was founded in 2006 by a group of Chinese dissidents and it came to prominence in 2009 and 2010 because of US government-related leaks.

- In 2010 the US government pressured banks and corporations to terminate payment and web-hosting services for WikiLeaks.

- WikiLeaks began to accept Bitcoin since July 2011 and has accumulated a small fortune from their Bitcoin holdings.

- Because of rape accusations and a threat of extradition to the US, Julian Assange fled to the Ecuadorian embassy in London in 2012.

- After he was expelled from the Ecuadorian embassy in April 2019, Assange was arrested and is incarcerated in a maximum security prison in Britain.

Decentralized WikiLeaks

- The arrest of Assange has resulted in a more decentralized WikiLeaks.
- 30 GB of the WikiLeaks document archive has been uploaded to the Interplanetary File System and links to WikiLeaks files are embedded in the Bitcoin Cash (BCH) blockchain.

  https://wikileaks.cash/
  ipfs://QmUmLnw5hp41zMpnCoMYH4SC2AJWpJW2KaJk5ENbzNUdpn
- The BCH blockchain also contains information to authenticate all the files on the IPFS, so that a user accessing the files can be confident that these were the original WikiLeaks files.
- Governments cannot prevent access to the files via the IPFS or prevent users from finding them (as long as IPFS and BCH exist).

Conclusions

- Blockchains or Distributed Ledger Technology (DTL) enables true decentralization of information and provides greater security than current methods of managing information.
- Decentralized blockchains offer strong censorship-resistance that can limit the ability of authorities to suppress undesirable information.
- Blockchains also enable the authentication of information that is decentrally stored to make sure that it has not been altered or tampered with.
- DTL will change the way information is stored and retrieved, emphasizing peer-to-peer interactions rather than centralized storage and control of information.

Thank You For Your Attention!

Armin Krishnan
East Carolina University
krishnana@ecu.edu