Bitcoin – Technical Features	Ethereum?
• Cryptography & Timestamped Logs	Yes
• Cryptographic Hash Functions	✓
• Timestamped Append-only Logs (Blocks)	✓
• Block Headers & Merkle Trees	✓✓
• Asymmetric Cryptography & Digital Signatures	✓
• Addresses	✓
• Decentralized Network Consensus	Yes
• Proof of Work	✓
• Native Currency	✓
• Network	✓
• Transaction Script & UTXO	No
• Transaction Inputs & Outputs	State Transitions
• Unspent Transaction Output (UTXO) set	Account Based
• Script language	7 languages

Source : MIT OpenCourseWare, https://ocw.mit.edu/ 15.S12 Blockchain and Money Fall 2018

Bitcoin vs Ethereum Design

• Founder: Satoshi Nakamoto	Vatalik Buterin
• Genesis: January 2009	July 2015
• Code: Non Turing (Script)	Turing Complete (Solidity, Serpent, LLL or Mutan)
• Ledger: UTXO – Transaction	State - Account Based
• Merkle Trees: Transactions	Transactions, State, Storage, Receipts (w/nonces)
• Block Time: 10 minutes	14 seconds
• Consensus: Proof of Work	Proof of Work
• Hash Function: SHA 256	Ethash

Source : MIT OpenCourseWare, https://ocw.mit.edu/ 15.S12 Blockchain and Money Fall 2018

Bitcoin vs Ethereum Design

• Currency: Bitcoin	⟷	ETH
• Mining: ASIC	⟷	GPU
• Hashrate: 54 Exahash/S	⟷	260 Terahash/S
• Pre-sale: None	⟷	ICO & prerelease of 72 m ETH
• Rewards: 12.5 BTC/block	⟷	3 ETH/block
• Monetary Policy: 1/2s every 210,000 blocks (4 yrs)	⟷	Fixed, but changes by updates (was 5/block; proposal to 2)
• Fees: Voluntary	⟷	Needed & market based

Source : MIT OpenCourseWare, https://ocw.mit.edu/ 15.S12 Blockchain and Money Fall 2018

Smart Contract Potential Use Cases

Digital Chamber of Commerce (12/16)

- Digital Identity
- Securities
- Derivatives
- Mortgages
- Supply Chain
- Clinical Trials

Records

Trade Finance

Financial Data

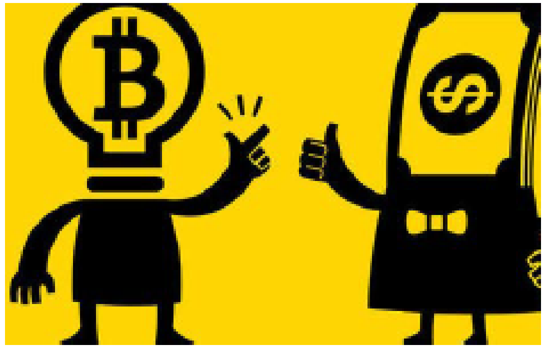
Land Title

Auto Insurance

Cancer Research

Source : MIT OpenCourseWare, https://ocw.mit.edu/ 15.S12 Blockchain and Money Fall 2018

Conclusions



- Nakamoto's P2P Money → Buterin's Ethereum P2P Computing
- Smart Contracts & DApps Provide:
  - Decentralized Computing &
  - Self Executing Commitments
- Token Sales for Proposed DApps have Spawned new form of Crowdfunding – Initial Coin Offerings (ICOs)
- Amongst 1000's of Proposals & Offerings, Few DApps have yet Gained Wide Consumer Adoption
- Smart Contracts and DApps, though, have real Potential to bring Change

Source : MIT OpenCourseWare, https://ocw.mit.edu/ 15.S12 Blockchain and Money Fall 2018