

# Blockchain

Gerald P. Dwyer

Clemson University

# Richard Branson

- Blockchain is an “Economic Revolution”



Source: CoinDesk, October 03, 2016

# Craig Pirrong

If you've been paying the slightest attention to financial markets lately, you'll know that blockchain is The New Big Thing.

Entrepreneurs and incumbent financial behemoths alike are claiming it will transform every aspect of financial markets.

The techno-utopianism makes me extremely skeptical.

Source: Craig's blog



# Pie in the Sky?



Source: shadowproof.com

**Price of Bitcoin based on Coindesk index  
September 1, 2013 to October 16, 2016**



# Computers

- “I see no reason why anyone would want a computer in their home.”
  - Kenneth Olsen, president of DEC, 1977

# Cray Supercomputer 1979



Source: Deutches Museum



# A 15-Times Faster Computer Today



Source: Samsung



# A Bit of Recent Press on Blockchain

- “UBS to build Blockchain-based trade finance system”
  - Wall Street Journal, September 29, 2016
- “J.P. Morgan has a new twist on blockchain.”
  - Wall Street Journal, October 3, 2016
- “Distributed ledger technology: Implications for payments, clearing, and settlement”
  - Lael Brainard, Board of Governors, October 7 2016

# IBM Survey of Financial Firms

- Fifteen percent of banks intend to implement full-scale, commercial blockchain solutions in 2017
- Roughly 65 percent of banks expect to have blockchain solutions in production in the next three years

Source: IBM press release, "Blockchain adoption ...", September 28, 2016

# IBM Survey of Financial Firms

- Fourteen percent of financial market institutions expect to have blockchain solutions in 2017
- Most early adopting financial market institutions are focusing their blockchain efforts on four areas
  - Clearing and settlement
  - Wholesale payments
  - Equity and debt issuance
  - Reference data

# What Is Blockchain?

- Blockchain can mean quite different things
  - Distributed ledger technology
  - Clear meaning in the context of Bitcoin

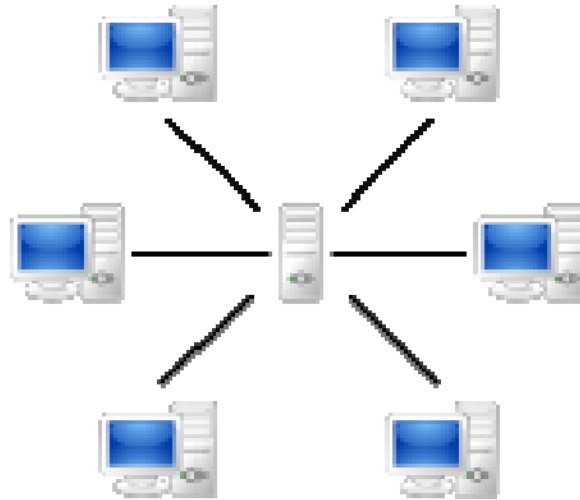
# Bitcoin and Blockchain

- The Bitcoin Blockchain is the major innovation that makes Bitcoin functional
- And it does make it functional

# Key Elements

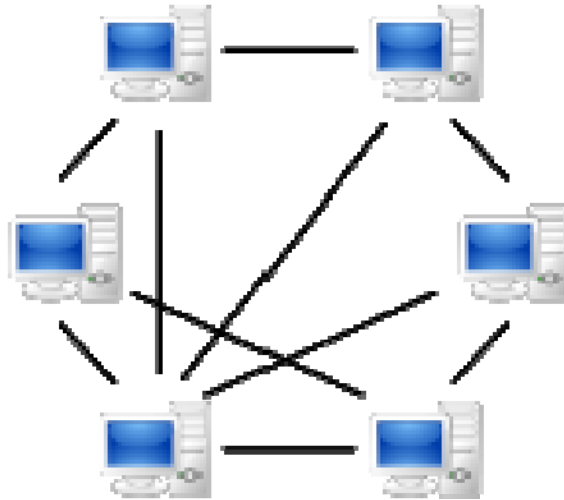
- Database of transactions
- Peer to peer network (distributed)
- Blocks are added to blockchain
- Consensus on current valid transactions

# Client-Server Network





# Peer-to-Peer Network



# Maintaining Record and Adding Transactions

- Why does anyone maintain the database?
  - Must be a payoff one way or another
  - Called “miners” in Bitcoin

# Consensus

- Consensus is agreement on the current correct set of transactions
  - Consensus need not be immediate
  - Consensus in Bitcoin is eventual

# Technical Background

- Blockchains involve hashes of records
- A hashing function reduces a message of some length to a shorter output

$$h = H(m)$$

- Highly nonlinear
- Not invertible

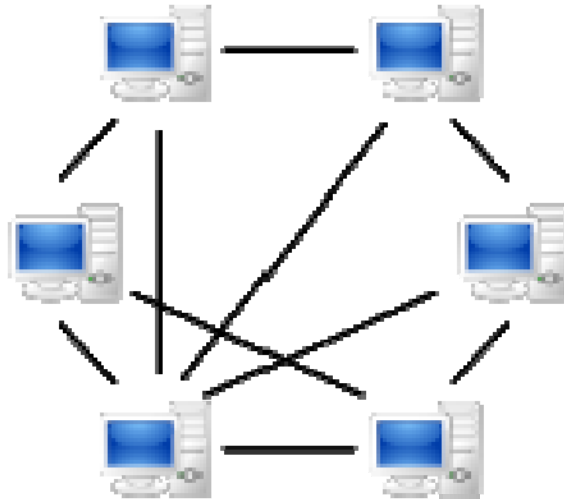
# Basic Elements of Blockchain

- Each block in the blockchain has a header
  - Address of miner receiving transaction fees and new bitcoins
  - Hash of previous block
  - Time stamp
  - Target “difficulty level” for hash of this block
  - Open field to alter hash (nonce)
    - Some other characters can be altered also

# A Block Includes Transactions

- Each transaction includes
  - Address to which bitcoins sent
  - Digital signature of party sending the bitcoins
    - Involves private-key cryptography
  - Number of bitcoins sent

# Peer-to-Peer Network





# Miners Add New Blocks

- Who adds a block?
- First “miner” who solves a numerical problem using a hashing function
  - Hard to solve numerical problem
  - Easy to verify it has been solved
  - Called “proof of work”
- Goal is to add a new block every ten minutes
  - Target difficulty level varied to make it so

# Miner Solves a Numerical Problem

- Compute hash of block's header which is less than or equal to a pre-specified value
  - Unique because transactions includes address of miner

$$h=H(m,nonce+other\ spaces)$$

- $h \leq$  pre-specified value
- *Nonce* is set of spaces that can be altered, leading to altered  $h$
- The effect of changing nonce on  $h$  is unpredictable

# Consensus about The Record of Transactions

- Consensus about transactions and solutions of mining problem
  - Verify transactions are valid
  - Longest chain is correct one
  - Eventual consensus on state
- Keep longest chain of transactions

# Consensus Background

- Byzantine Generals Problem
- Paper by Leslie Lamport and others laid out problem
  - Generals, spatially separated
  - Will others attack or not?
  - Important to follow the same plan

# Creating the Record of Transactions

- Miner who solves numerical problem gets
  - Newly created bitcoins
  - Transactions fees
    - Also motivates miners to include particular transactions

# Generalize?

- Record of transactions
- Establishes ownership

# Transactions and Ownership

- Financial markets
- Transfers between banks



# Other Possibilities

- Property registries
- Smart contracts
- Autonomous distributed organizations

# Pie in the Sky?



Source: shadowproof.com

# Japan Exchange Group Trial

- “Applicability of Distributed Ledger Technology to Capital Market Infrastructure”
  - Japan Exchange Group
  - IBM Japan Ltd.
  - Nomura Research Institute, Ltd.
  - CurrencyPort Limited
  - Participants from industry

# Trial

- Create a blockchain for clearing and settlement after trades
- Mainelli and Milne estimate \$40 billion a year in expenditures worldwide
  - Inconsistent private databases
  - Manual effort involved in clearing and settlement

# Blockchain Suggested

- Permission is required
- Consortium or “private”
- Consensus algorithm based on “Practical Byzantine Fault Tolerance”

# Practical Byzantine Fault Tolerance

- Approval of roughly  $2/3$  of nodes
- Tolerates errors in  $(n-1)/3$  of  $n$  nodes

# JPX Trail

- No proof of work
- Central party sends message on trades
- Uses smart contracts to settle
- Data privacy control
  - Can see own transactions, not others'
- Proof of ownership due to trusted third party
- Cash settlement after included in blockchain
  - Then finalized

# Overall Conclusions

- Tens to a hundred transactions per second
- Not currently feasible for high volume trading on exchanges
- Feasible for post-trade processing where millisecond and microsecond speeds are not necessary
- Sufficient for OTC trading
- Recommend central administrator with nodes mutually validating correctness of state
- Lower cost than current procedure



# Unresolved Issues

- Real time gross settlement of securities transactions

# Property Registry

- Hernando de Soto involved in an effort

# Smart Contracts

- Smart contract for escrow in Bitcoin
  - Multisignature initial transaction
  - Transfer to any party conditional on two of the three signatures

# Smart Contracts

- People have thought of more complicated contracts
  - Data dependent
    - Contracts for differences
    - Swaps

# Smart Contracts

- Pre-written logic (computer code)
- Stored and replicated on a distributed network
- Executed on a network of computers
- Can result in ledger updates

# Decentralized Autonomous Agents

- What does this mean?
- Bitcoin has been interpreted as a DAO

# Distributed Autonomous Agents



- M5 computer from Star Trek
  - Mercilessly attacked other ships

# Pie in the Sky?



Source: shadowproof.com



# Summary

- Blockchains are databases
  - Ledger of transactions
- Distinguishing aspect: peer to peer network
  - Sometimes called “Distributed ledger technology”
- Issue: Keeping consensus about correct entries with many different copies

# Summary

- Byzantine generals problem
  - Solution for Bitcoin not generally useful in other applications
  - “Practical Byzantine Fault Tolerance” is one alternative
- Privacy issues in some applications

# Possible Applications

- Clearing and settlement
  - Banks
  - Financial firms
- Wholesale payments
- Equity and debt issuance
- Reference data
- Property records

# Possible Applications

- Smart contracts
- Distributed autonomous organizations

# Research

- Serious policy issues
  - Disintermediation
  - Real time gross settlement
- Regulation
  - Small and large scale
- Theoretical
  - Organization around a blockchain and the implications for operation

# Research

- Bitcoin
  - Evasion of capital controls
  - Remittances
  - Calls for end of cash