Understanding Blockchain

Andrew Regenscheid
Computer Security Division
05.16.2018

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

"Explain to me how Bitcoin works." @JackGavigan
https://jackgavigan.com/2015/04/04/explain-to-me-how-bitcoin-works/

Prologue: Distributed Ledger Example

Alice and Bob playing Chess by Mail

- Alice sends Bob “1 e4”
- Bob sends back “1 ... e5”
- Alice sends Bob “2 Nf3”

If they don’t agree on the state of the board, they can’t play a game!

1. Both know the starting positions of the board.
2. Both know the sequence of messages so far (i.e., the moves)
3. Thus, they can reconstruct the state of the board.

If we agree on history, we agree on the present state of the world!

What's that got to do with Blockchain?

A blockchain lets us agree on the state of the system, even if we don't all trust each other!

- **Ultimate goal:** We all need to agree on the state of some system
  - How much BTC in each account?
  - Who owns which property?
  - What's the current state of my program?
- **We can all agree on that if we agree on history**
  - Starting state + history → current state
- **We don't want a single trusted arbiter of the state of the world**
  - We want some level of decentralization—not a single point of failure or compromise

Blockchain is…

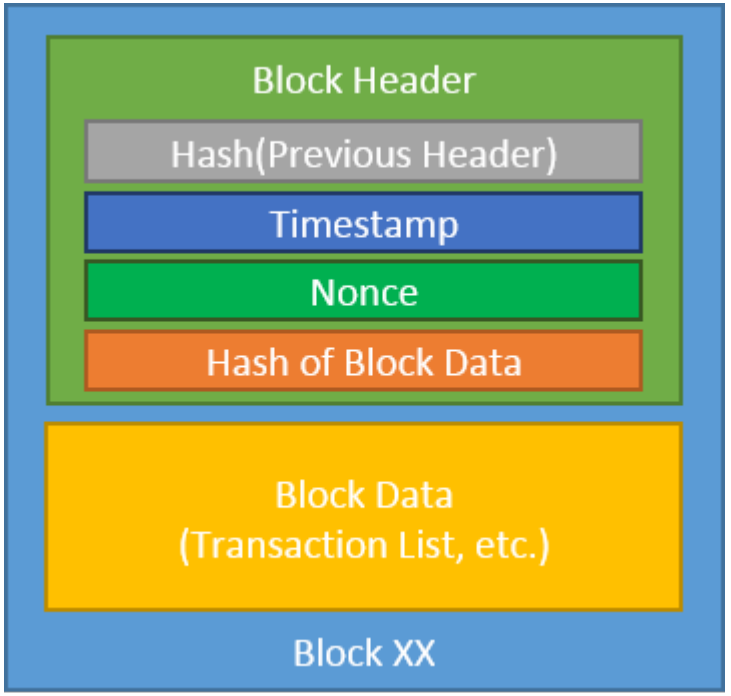
A **distributed ledger** which is:

- *Decentralized*
- *Peer-to-peer*
- *Tamper-evident/resistant*
- *Synchronized through consensus*

Facilitate transactions between mutually-distrusting entities without the need for a trusted arbiter

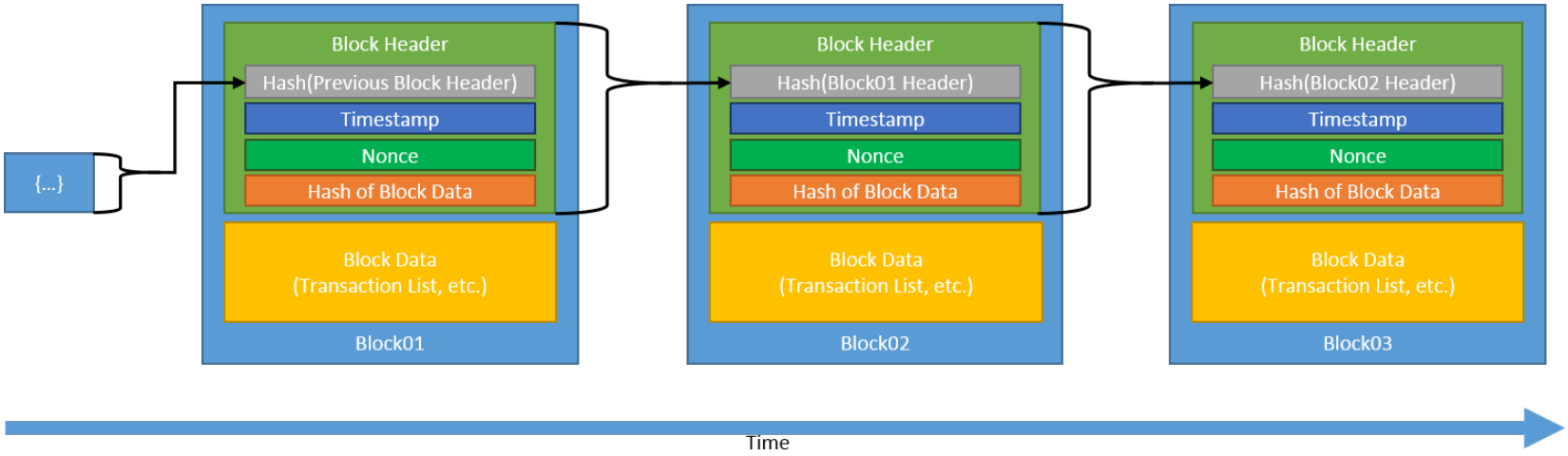
Blockchains- How do they work?

- Transactions are recorded in a sequence of blocks
- Linked together through a hash chain



Hash chains

- Blocks are cryptographically chained together
- A change in any block breaks the chain, providing tamper-evidence
- If the chain is broadly distributed, we can identify the valid chain, providing tamper-resistance



So, What's a Blockchain?

A blockchain is a sequence of hash-chained records along with:

- Validity conditions for new blocks
  - *Are transactions valid? Are digital signatures correct?*
- Defined procedures for adding blocks
  - *Who gets to add blocks? How is it done?*
- Consensus algorithms to agree on the state when conflicts arise
  - *When Alice and Bob have different pictures of history, there's some way for them to eventually come to agreement about who is right.*

NIST National Institute of Standards and Technology U.S. Department of Commerce

Blockchain Architectures

- **Permissionless blockchains**
  - Bitcoin
  - Ethereum
  - Zcash
- **Permissioned blockchains**
  - Hyperledger Fabric
  - Quorum

Permissionless Blockchains

Characteristics:

- Participation open to the **public**
- **Peer-to-peer** transactions
- Typically tied to **cryptocurrency**
- Fully **decentralized**

Challenges:

- **Privacy** and **scaling**

Permissionless blockchains are a disruptive technology that can dramatically change how we conduct business activities.

Permissioned Blockchains

Characteristics:

- Participation can be **private** and/or **controlled**
- **Trusted** participants
- More **efficient** than many public blockchains
- Can support **privacy** and **confidentiality** in transaction

Challenges:

- Some level of **centralized trust** through governing authority

Permissioned blockchains may lead to cost-savings, workflow improvements, automation and improved auditing with current business processes.

Case Study- Bitcoin

Bitcoin is the first decentralized digital currency, built on Blockchain technology.

- **Assets:** Bitcoin
- **Transactions:** payments between accounts

How does Bitcoin handle:

- *Validity conditions for new blocks?*
- *Defined procedures for adding blocks?*
- *Consensus algorithms to agree on the state when conflicts arise?*

Case Study- Bitcoin (1)

What are valid blocks of transactions?

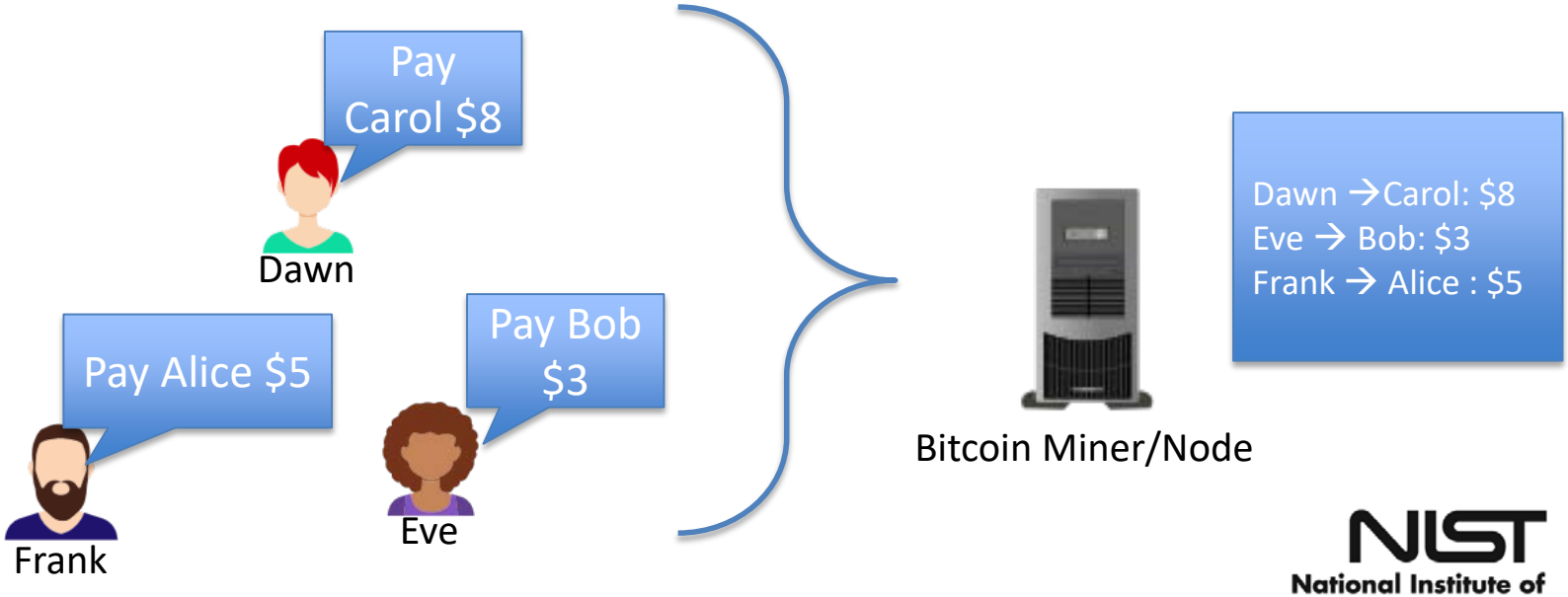
- Conditions
  - Transactions must be valid
    - Signatures needed for moving BTC from an account
    - Not allowed to leave a negative balance in an account
  - Block must contain a valid proof-of-work
- Anyone can verify the validity of a block
- A proposed block that doesn't meet these conditions won't be accepted by the rest of the network

Enforced by consensus

Case Study- Bitcoin (2)

Who can add a block?

- Transactions from Bitcoin users are broadcast to all nodes
- Nodes bundle these transactions in blocks
- Any node can add a block with a valid proof-of-work



National Institute of Standards and Technology
U.S. Department of Commerce

Proof-of-Work

- **Perform a big computation when adding blocks**
  - Expensive to perform by the proposing node
  - Cheap to verify by all others
- **Why is this useful?**
  - Limits the rate of new blocks
  - Makes attempts to add invalid blocks expensive
  - Provides a way to decide between competing chains- the chain with the most work wins

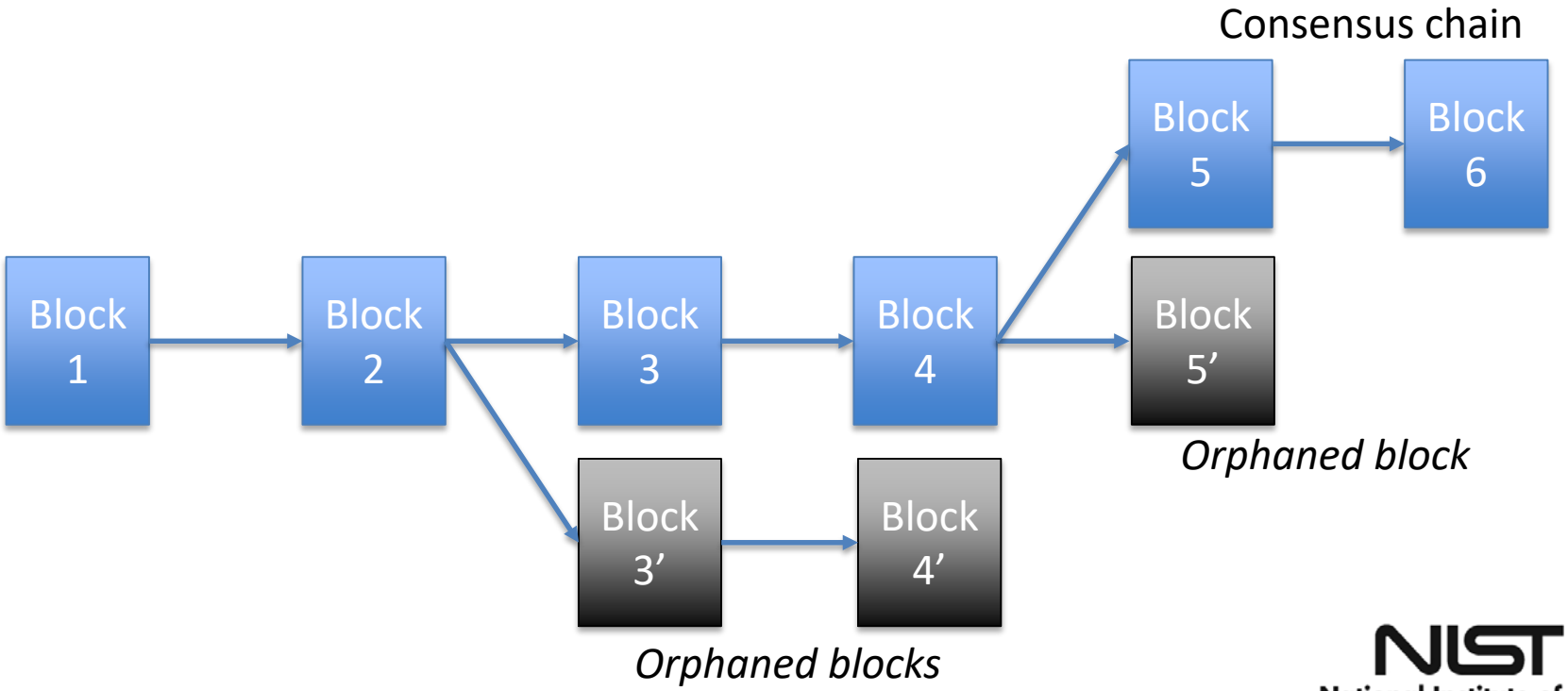
Bitcoin Mining

- **Mining:** the process of adding blocks to the Bitcoin blockchain
  - **Integral to bitcoin**: only way to add transactions
  - **Expensive**: must complete a proof-of-work per block
- **Mining Incentives:** The miner that adds a new block is paid:
  - **Mining Reward:** Currently 12.5 BTC
  - **Transaction Fees:** Small payments to miners from payers to incentivize inclusion of their transaction in a block
- **Miners are only rewarded if blocks are accepted**
  - Blocks containing invalid transactions will be rejected by other nodes
  - Strong incentive to play by the rules

Case Study- Bitcoin (3)

How do you settle disagreements?

When two or more valid chains exist, the longest chain wins



National Institute of Standards and Technology
U.S. Department of Commerce

Bitcoin Incentives

The real genius in Bitcoin's design is the way incentives are aligned:

- Untrusted, self-interested miners keep the system working
- They have a big incentive to follow the protocol
- They have substantial capital invested in Bitcoin, so they also have an incentive to avoid any attack that would undermine their investment

Public blockchains must have carefully balanced incentives to incentivize honest behavior and converge on a consensus.

How Else Could it Work?

Permissioned Blockchains

Scenario: *Closed community with many users and 5 trustees*

- **Validity Conditions for New Blocks:**
  - Are transactions well-formed?
  - Has ownership between established?
- **Who can Add Blocks:**
  - Transactions in blocks verified by trustees
  - A block accepted to the chain with a 3/5 vote of trustees
- **Resolving Conflicts:**
  - Chain with the most votes wins

Many variations possible with different roles, permissions, validity conditions, and consensus algorithms.

Use Cases- What can I do with Blockchain?

Depending on who you ask, everything…

Expectations

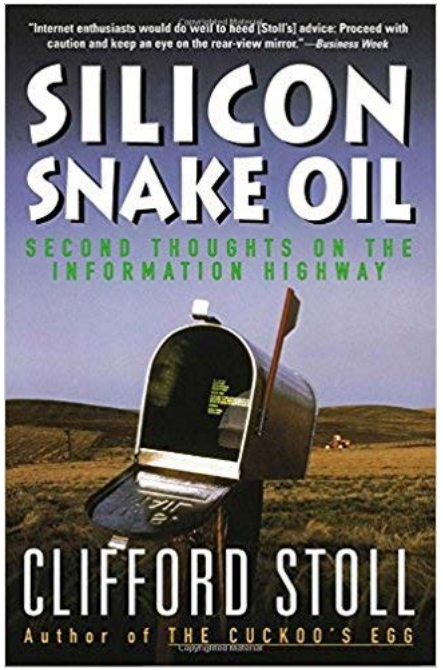
"Long Island
much as 289
rebranded its

National Institute of Standards and Technology
U.S. Department of Commerce

Careful with Predictions…

"Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems. And the freedom of digital networks will make government more democratic.

Baloney. Do our computer pundits lack all common sense?" [emphasis added]



Clifford Stoll, *Why the Web Won't Be Nirvana*, Newsweek. 2/26/1995.

NIST National Institute of Standards and Technology U.S. Department of Commerce

What do blockchains give us?

- **A distributed, immutable chain of records**
- **Methods to own and transfer assets**
  - Native assets (cryptocurrency), digital assets, or digital representations of physical assets
- **Automation of business processes through smart contracts**
  - Transactions are small programs that execute on blockchain nodes
- **Decentralized trust**

Use Cases

- Financial services
- Land/property records
- Identity management
- Supply chain management

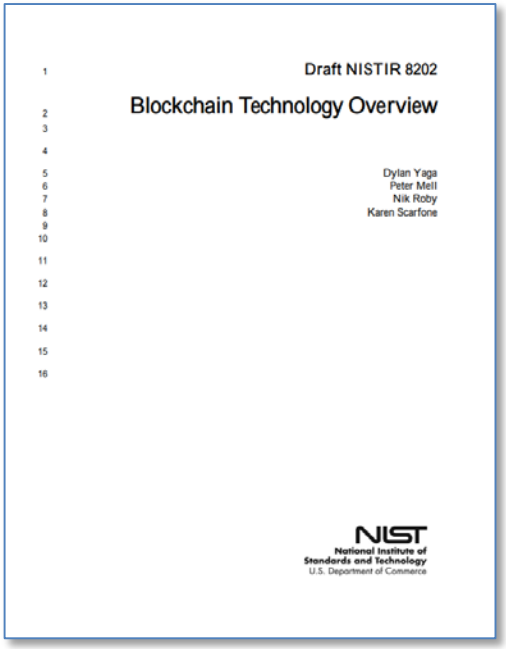
And many, many more…

Considerations

	Permissionless Blockchains	Permissioned Blockchains
Advantages	• **Fully decentralized** • **Strong notion of tamper-resistance/immutability** • **Builds upon existing public infrastructure**	• **Distributed trust** • **Permission models provide greater control** • **Typically more efficient, supports greater throughput, faster transaction times** • **Full control over governance**
Disadvantages	• Slow transaction confirmation times • Limited throughput for on-chain records • Transaction details may be public- *But emerging technologies are working to address that* • Open governance model	• Reliance on central trust authority • May require dedicated infrastructure

Draft NISTIR 8202 – Blockchain Technology Overview

- Released for Public Comment Period January 24, 2018 to February 23, 2018
- Provides a high level overview of:
  - The underlying technologies:
    - Cryptographic Hash Algorithms
    - Asymmetric Key Cryptography (Public Key Cryptography), and Digital Signatures
  - The mechanics of a blockchain (generalized)


Draft NISTIR 8202

Blockchain Technology Overview

Dylan Yaga
Peter Mell
Nik Roby
Karen Scarfone

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8202 – Blockchain Technology Overview

- The document also touches on:
  - Consensus algorithms
  - Soft and Hard forks of blockchain technology
  - Smart Contracts
  - Categorization (e.g., permissioned, permissionless, public, private)
  - Considerations for use
  - Some misconceptions we have been asked about/heard
  - Small overview of some of the blockchain landscape

Questions?

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov

Dylan Yaga

Dylan.Yaga@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

Backup Slides

Use Case- Financial Services

- **Decentralized Cryptocurrency** use case naturally extends to other assets
- Financial services
  - Could greatly reduce time to clear complicated financial instruments
  - Current processes often involve many parties and counterparties
- Land records
  - Record land records on public or private blockchains
  - Could cut transaction and record-keeping costs, improve accuracy, and reduce fraud

Use Case- Identity Management

- **Blockchain immutability could support identity trust infrastructures**
  - Blockchain technologies could record/share identity attributes
  - Identities for people/devices could be recorded on a blockchain
- **Assets:** Identity attributes, identifiers
- **Transactions:** Establishing or using attributes, identifiers
- **Blockchain as a trust anchor**
  - Identify and authenticate users off-chain, using data that can be verified using the blockchain

Use Case- Supply Chain Management

- **Use blockchain to track components through their lifecycle**
  - Manufacturing, integration, sale, and use
- **Assets:** Components
- **Transactions:** Sale/transfer of components between suppliers/vendors
- **Potential Benefits**
  - Transparency of the supply chain
  - Immutability of the path