Information Technology Fundamentals

Mohammad Hossein Manshaei
manshaei@gmail.com

Web Systems: Blockchain and Cryptocurrency
Module 5: Part 8

Module 5. Main Objectives

1. Review Web System Architecture
2. Explain E-Commerce Business Models
3. Review Recommender Systems
4. **Describe Blockchain Systems, Cryptocurrency, and Smart Contracts**

Introduction to Cryptocurrencies & Blockchains

Main Reference

Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. ***An Overview of Blockchain Technology, Architecture, Consensus, and Future Trend,*** *IEEE 6th International Congress on Big Data*, 2017

2017 IEEE 6th International Congress on Big Data

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Zibin Zheng[1], Shaoan Xie[1], Hongning Dai[2], Xiangping Chen[4], and Huaimin Wang[3]

[1]School of Data and Computer Science, Sun Yat-sen University Guangzhou, China
[2]Faculty of Information Technology, Macau University of Science and Technology, Macau, SAR
[3]National Laboratory for Parallel & Distributed Processing
National University of Defense Technology, Changsha 410073 China
[4]Institute of Advanced Technology,National Engineering Research Center of Digital Life
Sun Yat-sen University, Guangzhou, China
Email: zhzibin@mail.sysu.edu.cn

***Abstract*—Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.**

***Index Terms*—Blockchain, decentralization, consensus, scalability**

I. Introduction

Nowadays *cryptocurrency* has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 [1]. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is *blockchain*, which was first proposed in 2008 and implemented in 2009 [2]. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve

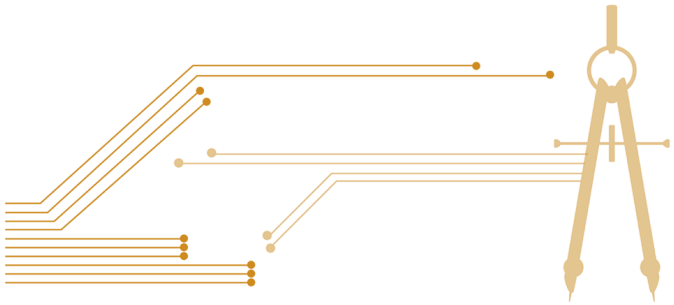
Things (IoT) [7], reputation systems [8] and security services [9]. Those fields favor blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain.

Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading. However, larger blocks means larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large blockchain. Therefore the tradeoff between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy [10]. Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders blockchain development. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage could also happen in blockchain even users only make transactions with their public key and private key [11]. Furthermore, current consensus algorithms like *proof of work* or *proof of stake* are facing some serious problems. For example, proof of work wastes too much electricity energy

Main Reference

M. Crosby et al.
Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2016

Applied Innovation Review Issue No. 2 June 2016



BlockChain Technology: Beyond Bitcoin

Authors:
Michael Crosby (Google)
Nachiappan (Yahoo)
Pradan Pattanayak (Yahoo)
Sanjeev Verma (Samsung Research America)
Vignesh Kalyanaraman (Fairchild Semiconductor)

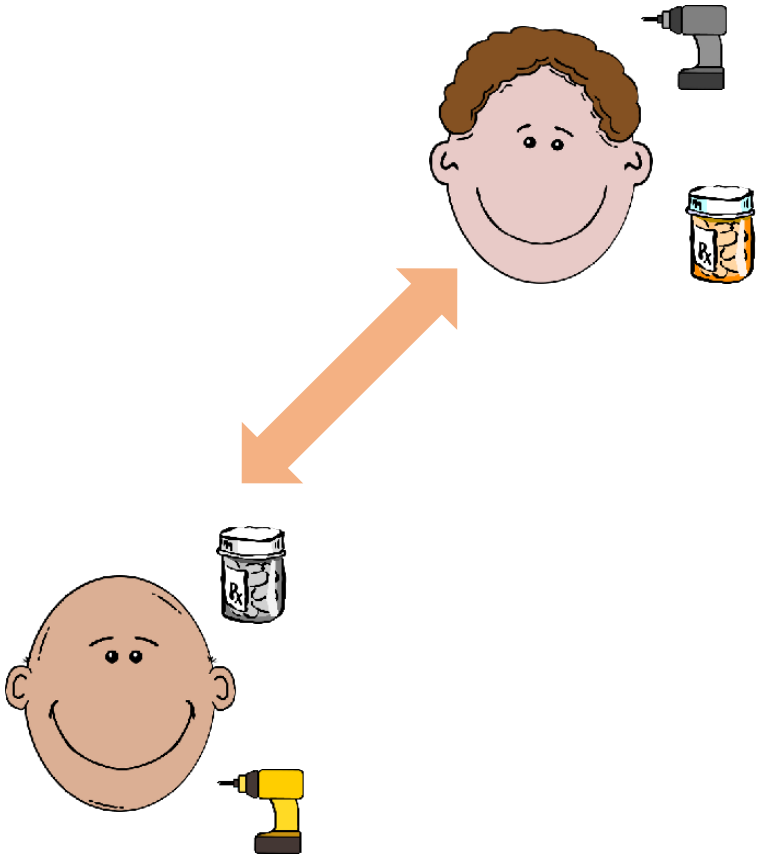
Contents

- Motivation: E-Cash, Credit, Digital Currency, CryptoCurrency, …
- Public Ledger and Blockchain
- BitCoin: Main Idea and Framework
  - ✓Transactions
  - ✓Proof of Work
  - ✓Attacks and Trust
  - ✓Block Reward
- Smart Contract: A Blockchain Approach

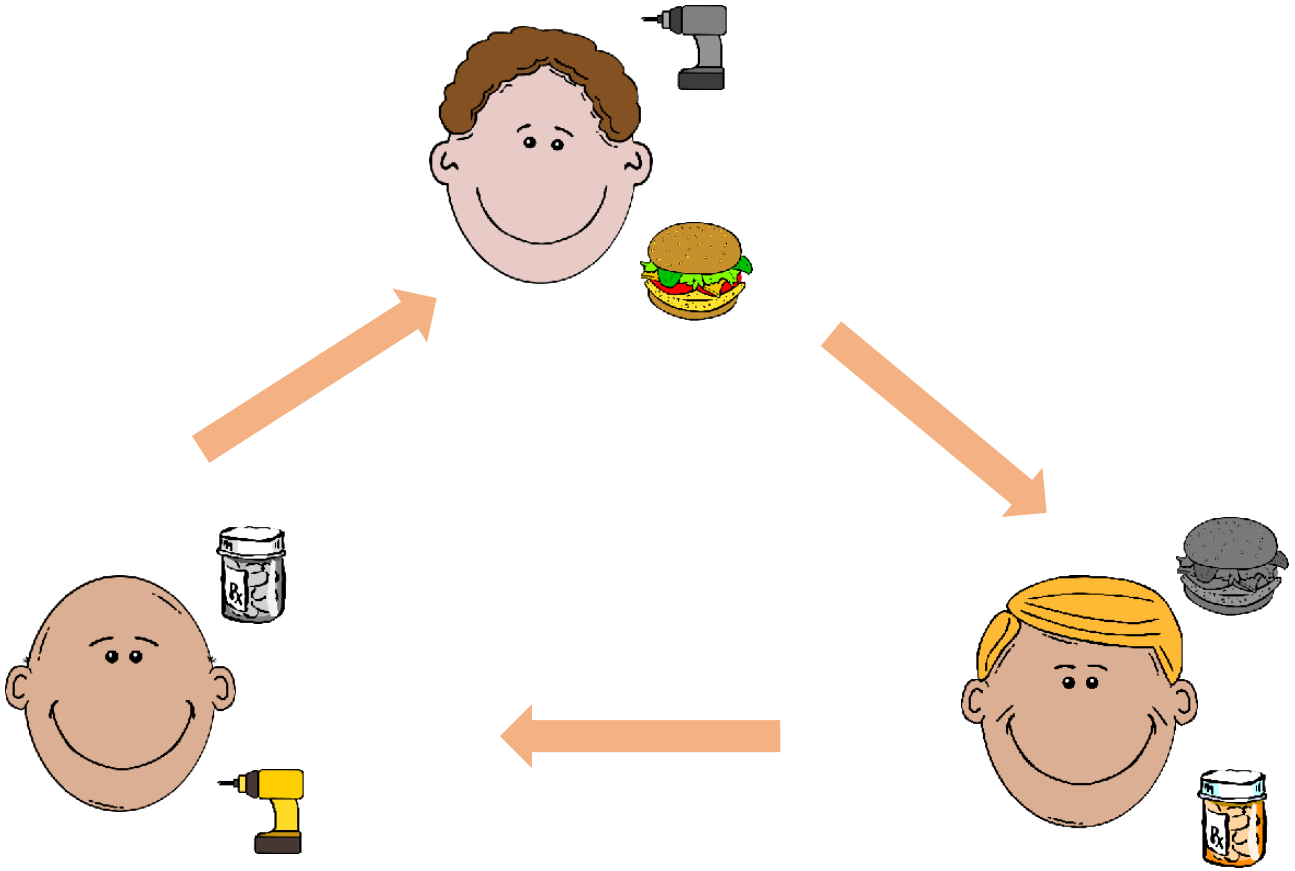
Traditional Currencies

1. Barter
2. Credit
3. Cash

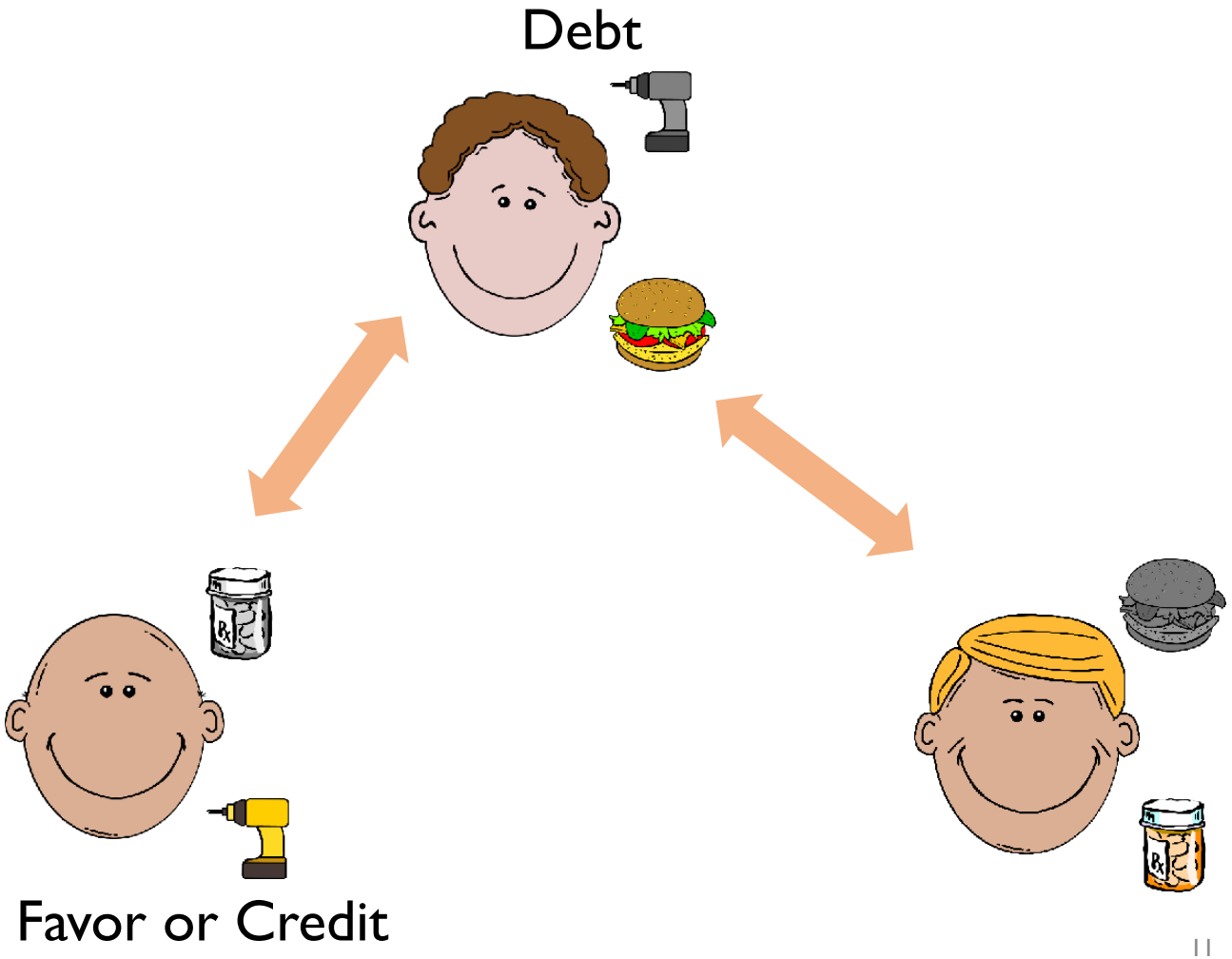
Barter



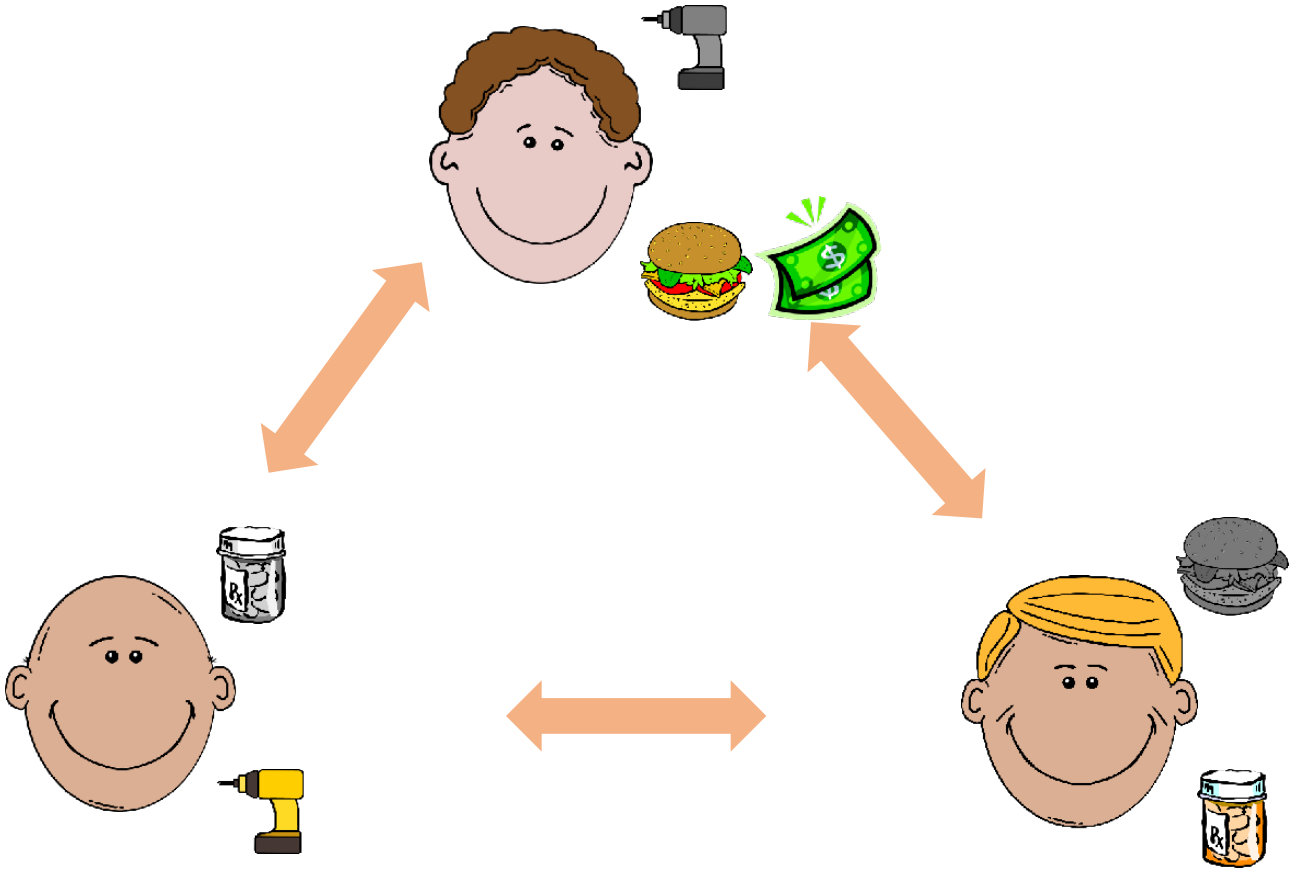
Barter



Credit



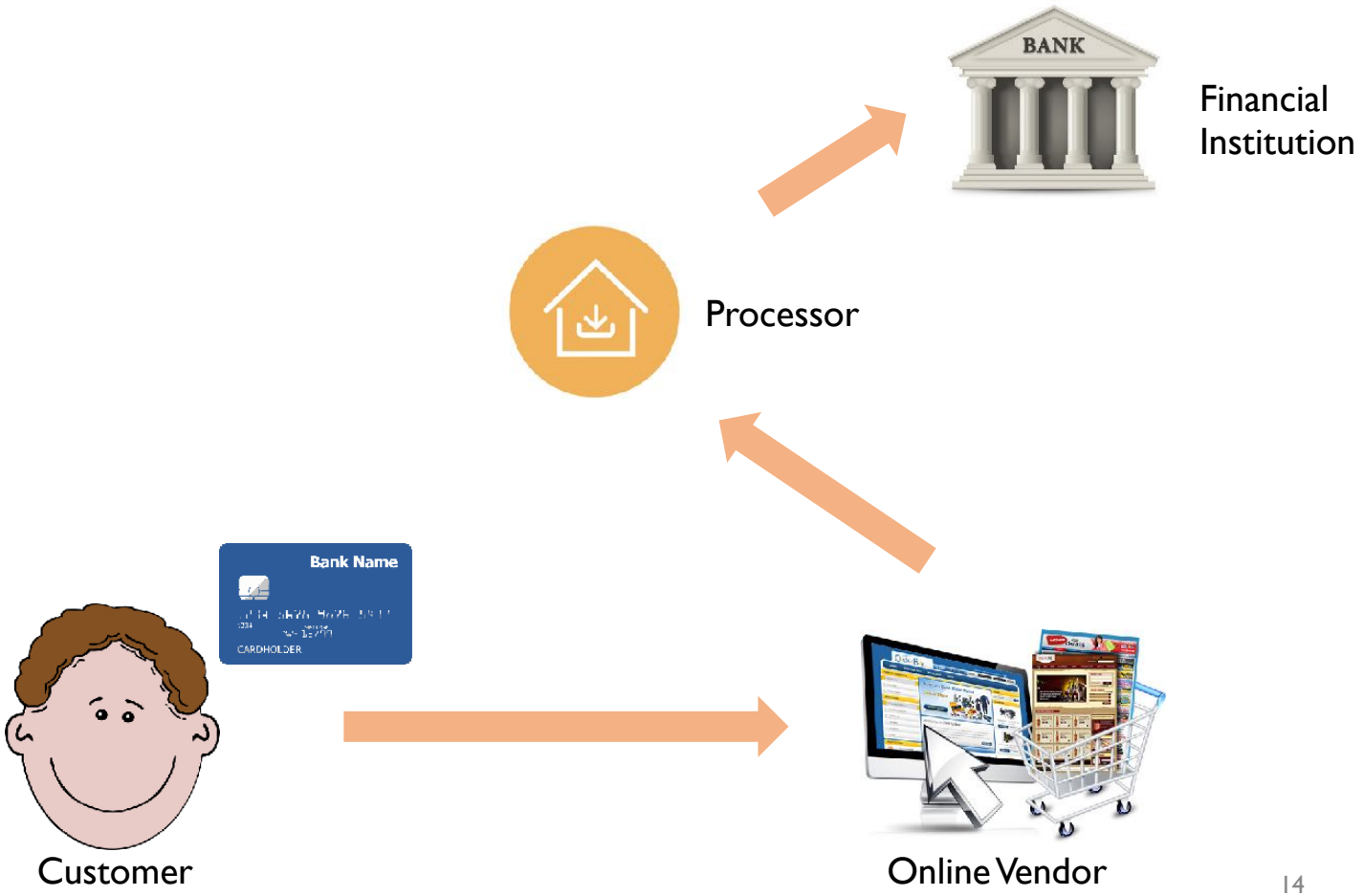
Cash



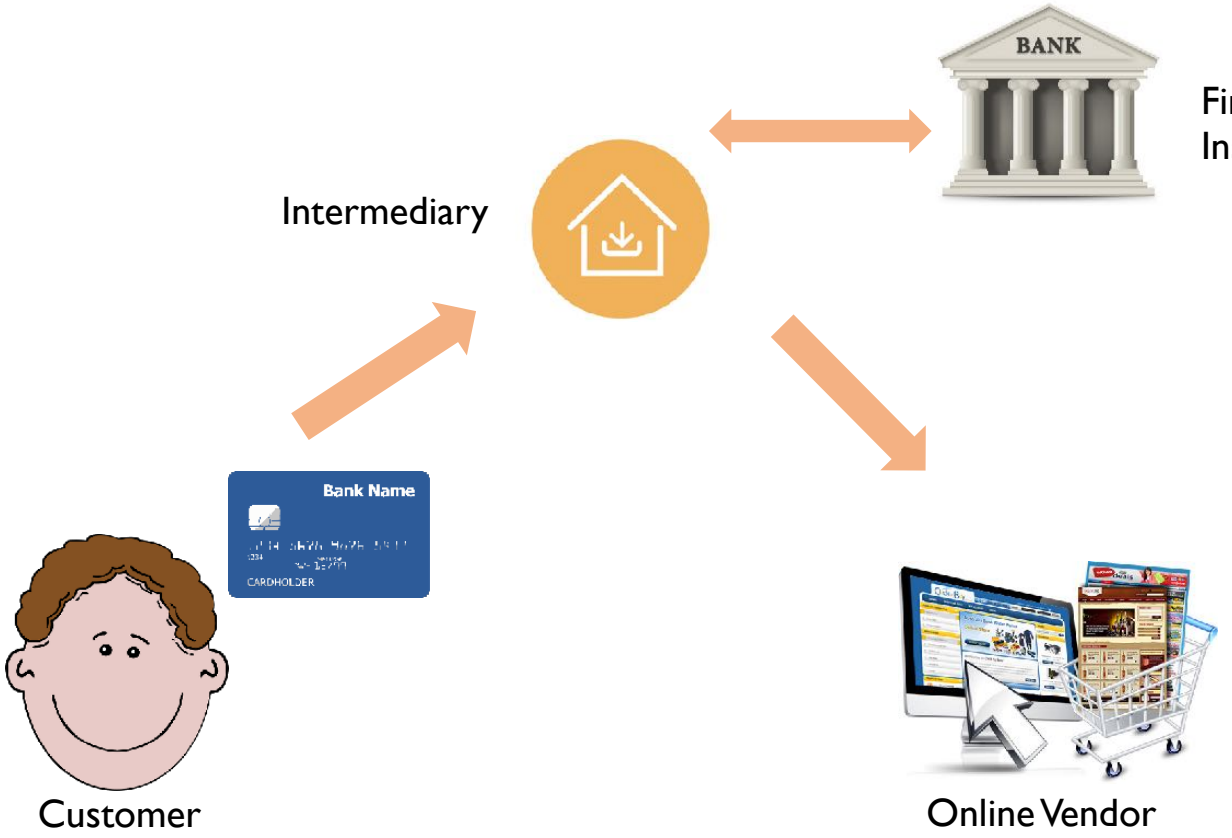
Cash vs Credit

- Cash requires initial allocation, but allows fine-grained valuation of products
- Credit acquires risk
- When cash and credit are combined?
  - Cash allow credit to be quantified, for example, how much a person owes another?

Digital Credit Architecture I



Digital Credit Architecture 2



Advantages: Hides customer credit card data from online vendors.
Disadvantages: Requires redirection, enrollment, etc.

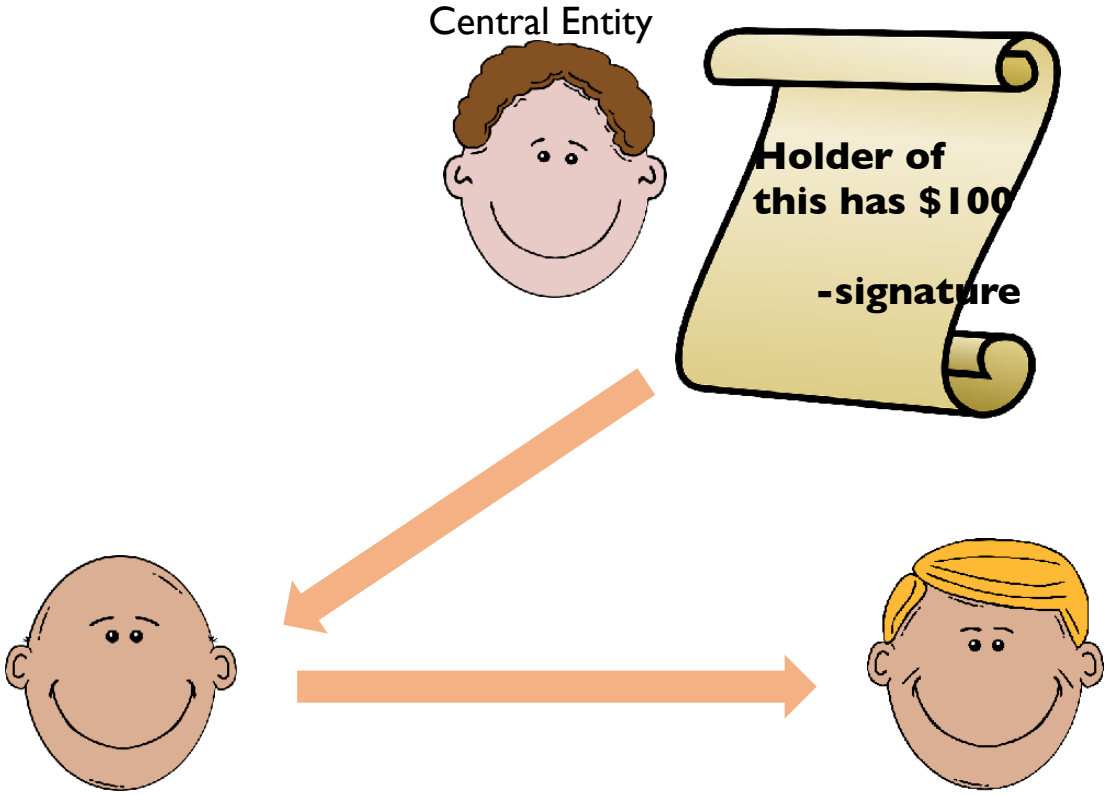
Digital Cash

- In parallel, there has been a lot of research in cash-like systems.

- Ideal Requirements:
  - Higher anonymity (similar to traditional fiat cash).
  - Offline transactions.

First Proposal for eCash

- David Chaum (1983)



Problems with Chaum's Scheme?

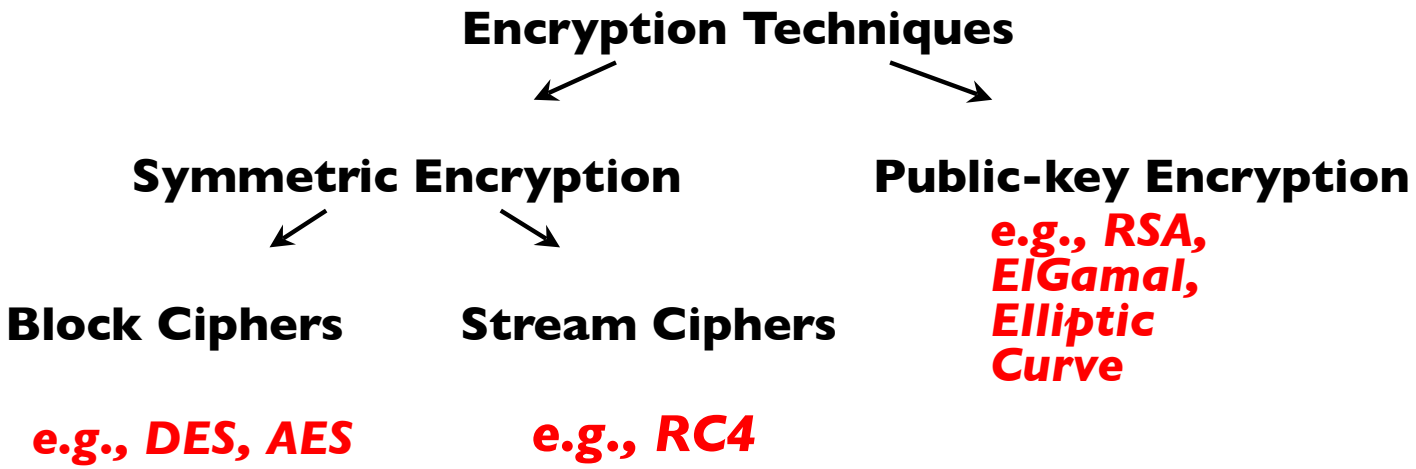
Copying and double spending is easy!

1. First attempt to fix: Introduce *serial numbers*.
   - Shortcoming: Traceability!

2. Second attempt to fix: use *Blind Signatures*.
   - Shortcoming: Requires a centralized entity that records and maintains all transactions!

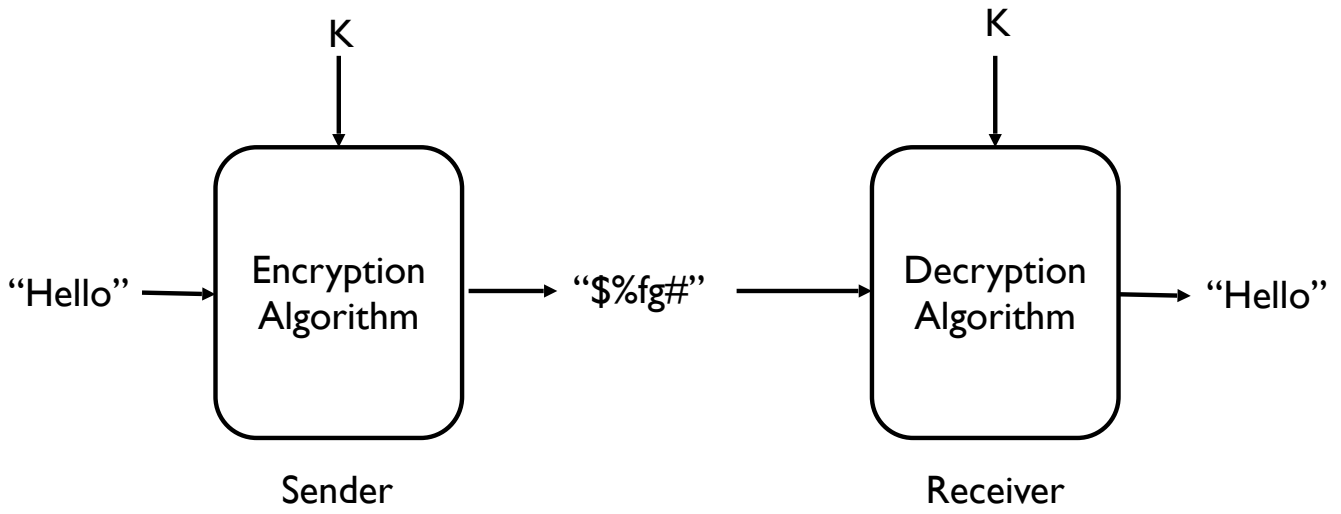
Encryption

Process of transforming information (a.k.a plaintext) into something that is unintelligible (a.k.a ciphertext) to everyone except authorized receivers.



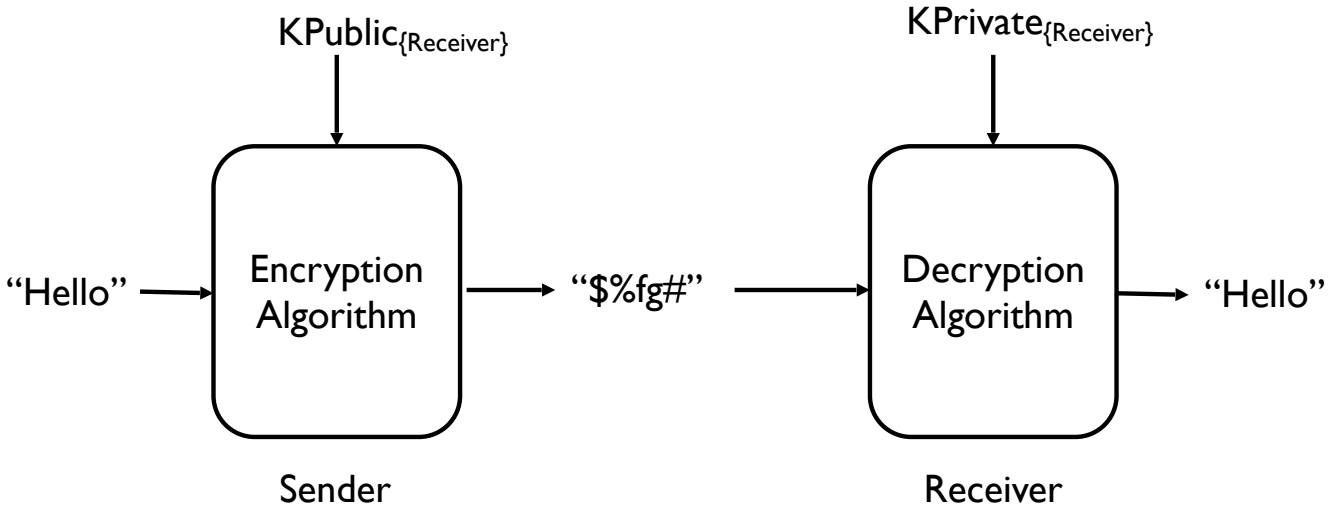
Symmetric Encryption

Algorithm uses the same key for encryption and decryption - also referred to as single-key encryption.

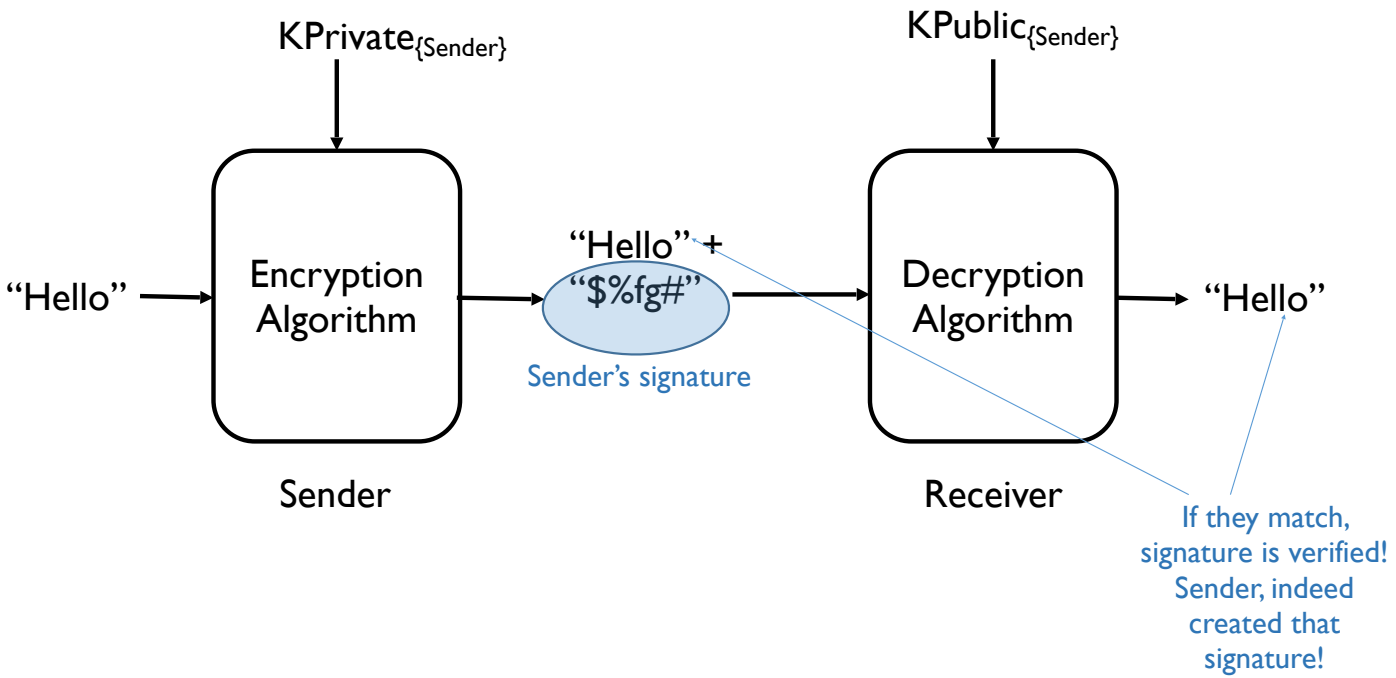


Public-Key Encryption

- **Asymmetric** - uses two separate keys:
  - Public key is made public for others to use.
  - Private key is secret and is never released.



Digital Signatures



Why?

Only sender knows his/her private key ? Only sender can create signature, anyone can verify!

Digital Signature Properties

Same as properties we need from handwritten signatures:

1. Security: only you can sign as yourself, but anyone can verify that your signature was indeed made by you.

2. Unforgeability: signature tied to a particular document - can't be cut-and-pasted to another document.

Drawbacks

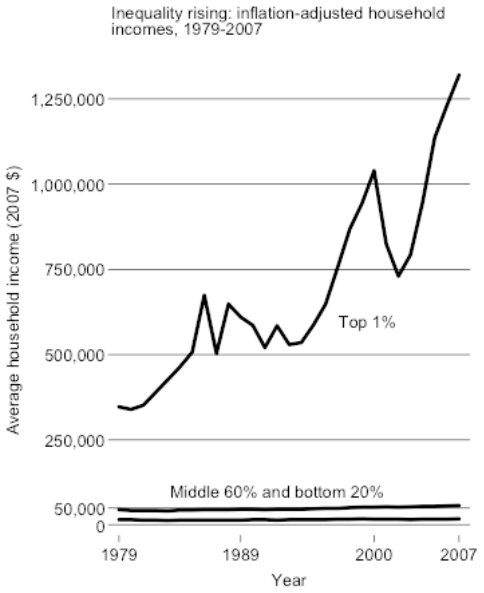
- Drawbacks of current digital currency systems:
  1. Most require a centralized trusted entity.
  2. Some require specialized hardware.
  3. Some require complex/specialized cryptographic techniques.
  4. Others do not provide enough privacy/ anonymity.

Motivation

- How can we design a new form of digital currency that
  - does not require a centralized entity, and,
  - does not require a specialized hardware, and,
  - does not require complex cryptography, and,
  - provides decent anonymity?

This was the main motivation that led to the development of Bitcoin!

A Little Bit of Politics!!



Contents

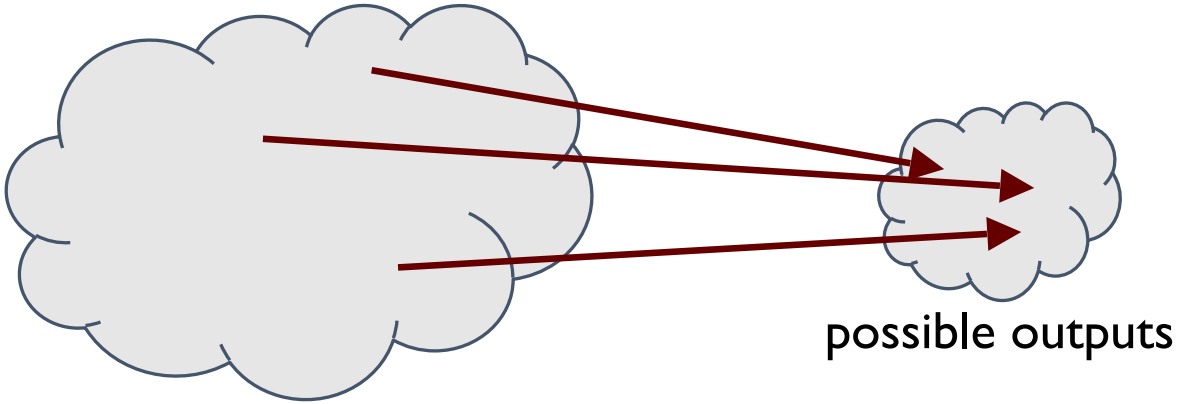
- Motivation: E-Cash, Credit, Digital Currency, CryptoCurrency, …
- Public Ledger and Blockchain
- BitCoin: Main Idea and Framework
  - ✓Transactions
  - ✓Proof of Work
  - ✓Attacks and Trust
  - ✓Block Reward
- Smart Contract: A Blockchain Approach

Key Enabler

- How to create and maintain an append-only, immutable record or ledger of transactions
  - in a *distributed fashion* without requiring any centralized entity, and,
  - without requiring any *specialized hardware*, and,
  - without requiring *complex cryptography*, and,
  - such that it provides *user anonymity*?

- Result: Bitcoin P2P network that maintains transactions on the Blockchain!

Hash Functions



All hash functions satisfy the following properties:

1. Inputs can be any size (not-fixed).
2. Outputs are fixed-size (output size <= input size).
3. Efficiently computable.

Cryptographic Hash Functions

Satisfy the following additional security properties:

1. Collision Resistance: Infeasible to find *x* and *y* such that *x* != *y* and H(*x*)=H(*y*)

2. Hiding or Pre-image Resistance: Given H(*r* | *x*) and *r*, where *r* is random, it is infeasible to find x.

3. Puzzle-friendliness: Given a *y* such that H(*k* | *x*) = *y*, and *k* is random and known, it is infeasible to find *x*.

Hash Function Applications

1. Message digest: Verify integrity of data (i.e., whether the data under question has changed).

2. Commitments: Commit to a value, reveal it later (analogous to sealing something in an envelope)

3. Search Puzzles:

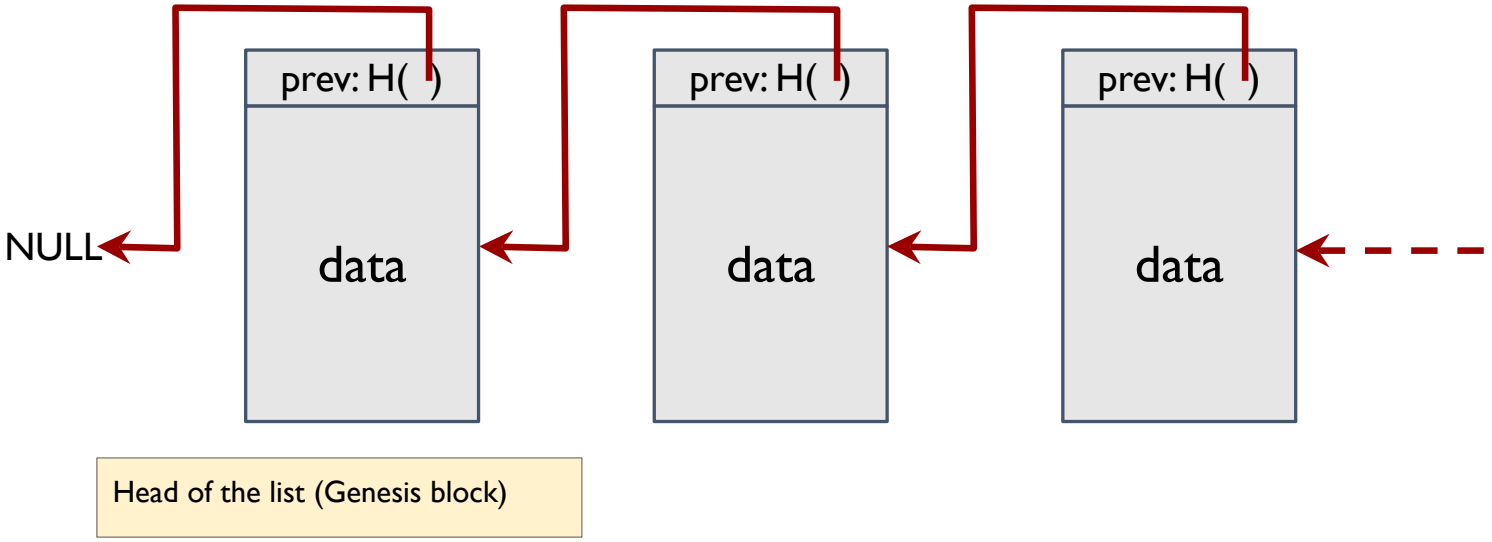
Given: A random "puzzle ID" *id* and a target set *Y*:

Objective: Try to find a "solution" *x* such that $H(id \mid x) \in Y$.

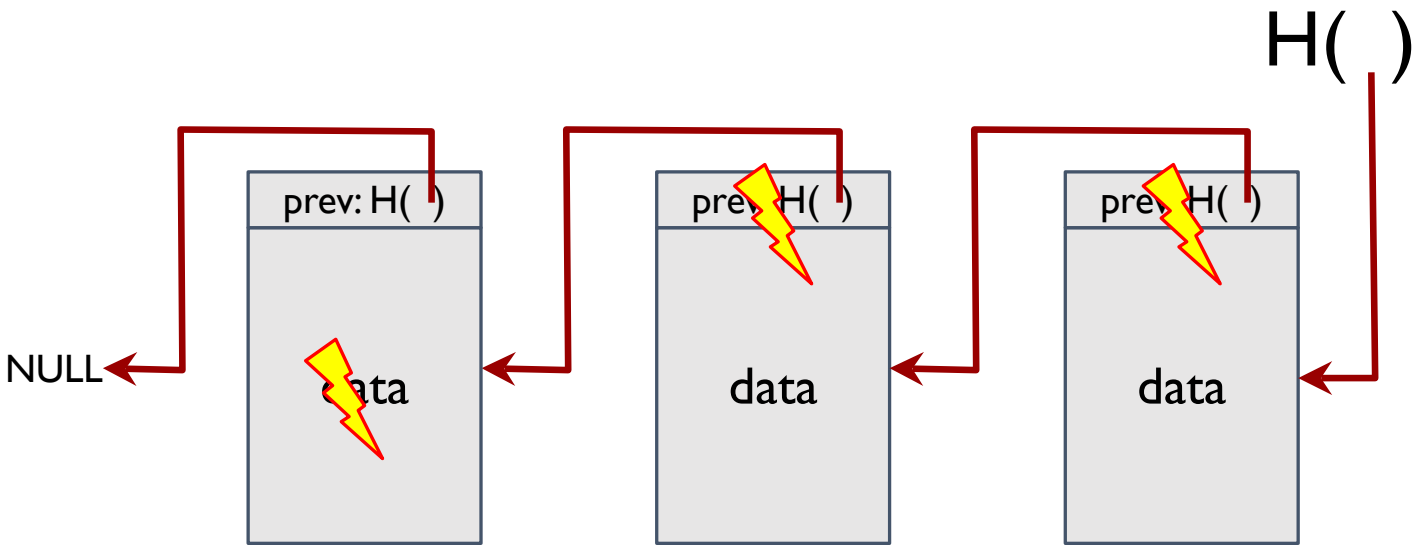
Puzzle-friendly property implies that no solving strategy is much better than trying random values of x.

Blockchains

- What is a Blockchain?
  - Linked or ordered list of hash pointers and data blocks.
- What is it used for?
  - Tamper-evident log or register



Tamper-evident Log



Contents

- Motivation: E-Cash, Credit, Digital Currency, CryptoCurrency, …
- Public Ledger and Blockchain
- BitCoin: Main Idea and Framework
  - ✓Transactions
  - ✓Proof of Work
  - ✓Attacks and Trust
  - ✓Block Reward
- Smart Contract: A Blockchain Approach

What is Bitcoin?

Digital cash or financial instrument:

- Proposed in 2009 by an anonymous author under pen name "**Satoshi Nakamoto**" on the cypherpunks mailing list.
- Is managed in a completely distributed manner.
  - No central authority or government controls Bitcoins.
- Can be (and is) used for online and other transactions and to settle debts.
- Can be (and is) exchanged for other fiat currency.
  - By means of Bitcoin exchanges.
- Can be (and is) traded as other fiat currency.
  - It is what gives Bitcoins its value!

Bitcoin Summary

- A purely distributed system that records and maintains an immutable and consistent ledger (a.k.a. Block chain) of transactions.

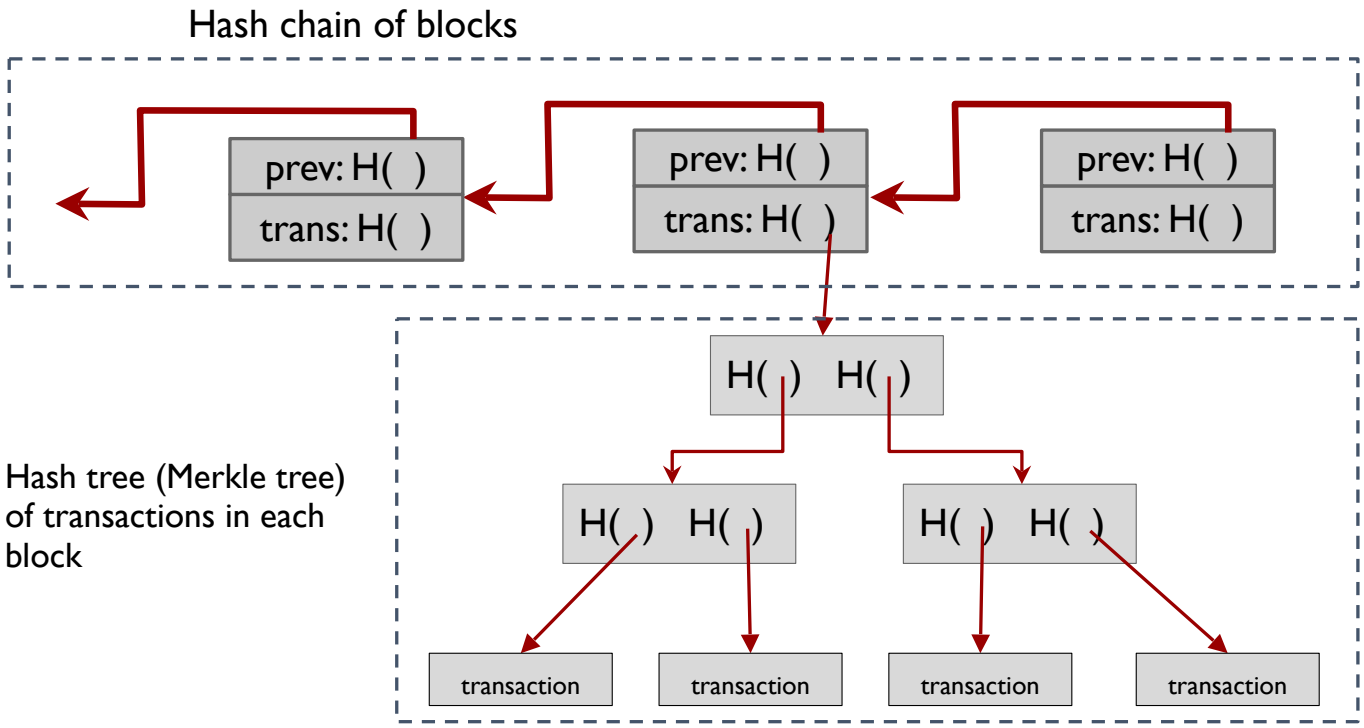
- Three Important Aspects of Bitcoins:
  1. Data structures: *what is stored in these ledgers*?
  2. Bitcoin peer-to-peer network: *who maintains these ledgers*?
  3. Consensus: *how is the consistency and immutability of these ledgers maintained*?

Bitcoin Blocks

- In a Bitcoin system, multiple transactions are bundled together in blocks.
  - Rather than recording individual transactions into the ledger (or Blockchain), the system records blocks

- Why bundle transactions together?
  - Efficiency!

Bitcoin Block Structure



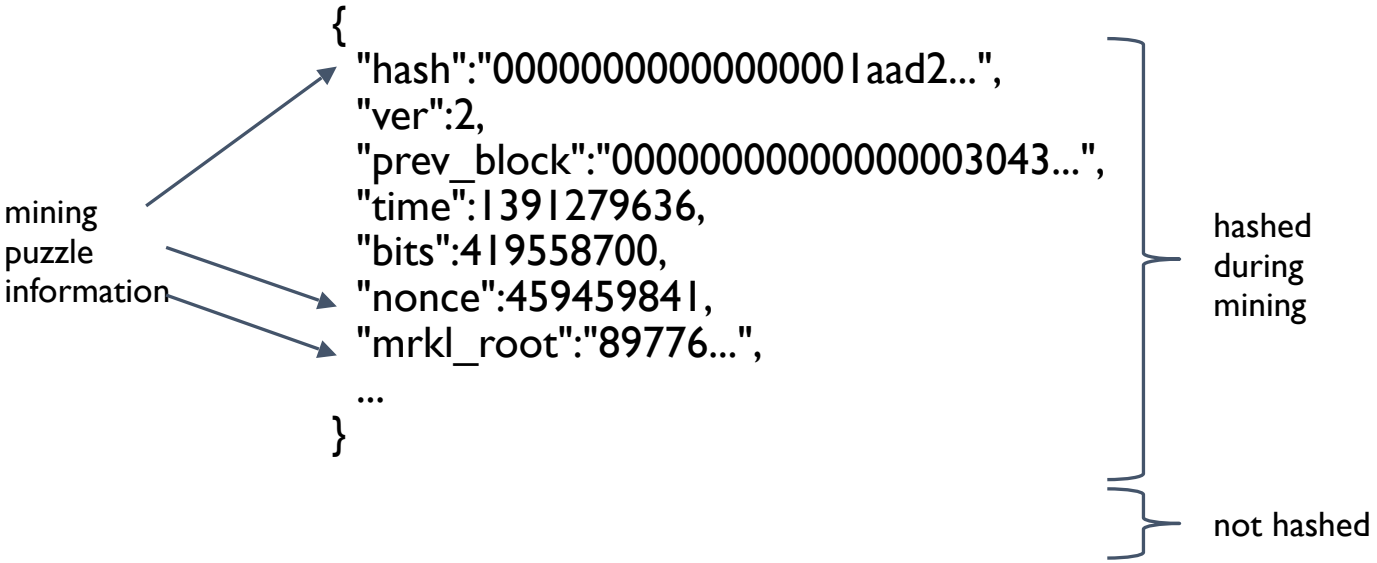
A Bitcoin block

Block header

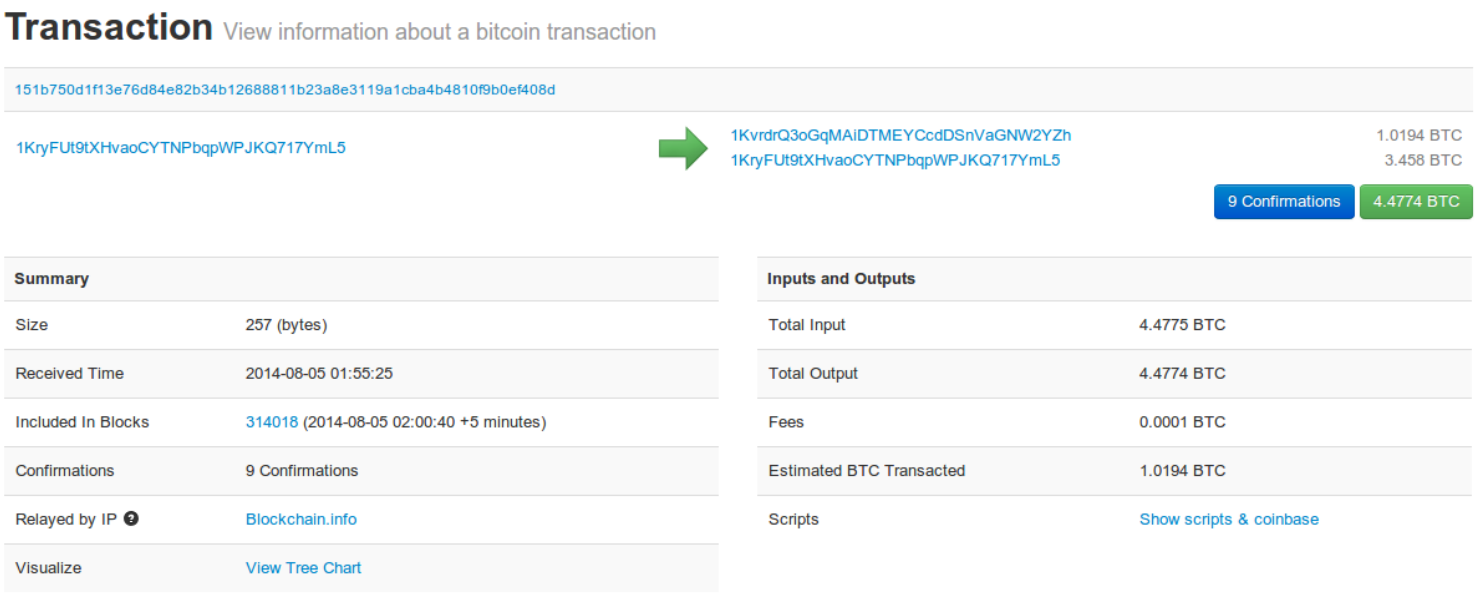
Transaction data


```
{
  "hash":"0000000000000000001aad2...",
  "ver":2,
  "prev_block":"0000000000000000003043...",
  "time":1391279636,
  "bits":419558700,
  "nonce":459459841,
  "mrkl_root":"89776...",
  "n_tx":354,
  "size":181520,
  "tx":[
    ...
  ],
  "mrkl_tree":[
    "6bd5eb25...",
    ...
    "89776cdb..."
  ]
}
```

A Bitcoin block header



See for Yourself!



Transaction View information about a bitcoin transaction

151b750d1f13e76d84e82b34b12688811b23a8e3119a1cba4b4810f9b0ef408d

1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5	1KvrdrQ3oGqMAiDTMEYCcdDSnVaGNW2YZh	1.0194 BTC
	1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5	3.458 BTC

9 Confirmations | 4.4774 BTC

Summary	
Size	257 (bytes)
Received Time	2014-08-05 01:55:25
Included In Blocks	314018 (2014-08-05 02:00:40 +5 minutes)
Confirmations	9 Confirmations
Relayed by IP	Blockchain.info
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	4.4775 BTC
Total Output	4.4774 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	1.0194 BTC
Scripts	Show scripts & coinbase

blockchain.info (blockexplorer.com, or many other sites)

Bitcoin P2P network

- Nodes run a Bitcoin reference (or other) client on TCP port 8333 implementing an ad-hoc communication protocol.

- Nodes typically:
  - Create transactions
  - Forward transactions
  - Validate transactions
  - Add transaction blocks onto the Blockchain

- Ad-hoc network has random topology – no centralized coordinating service or authority

- All nodes are equal – however two types of nodes typically found:
  - Fully validating nodes
  - Thin clients or SPV nodes

- New nodes can join any time - forget non-responding nodes after 3 hours

How big is the Bitcoin network?

- Impossible to measure exactly.
- Estimates - up to 1M new IP addresses/month. (2015)
- Only about 5-10k "fully validating nodes"
  - This number may be dropping!