Cryptocurrencies & Blockchains

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

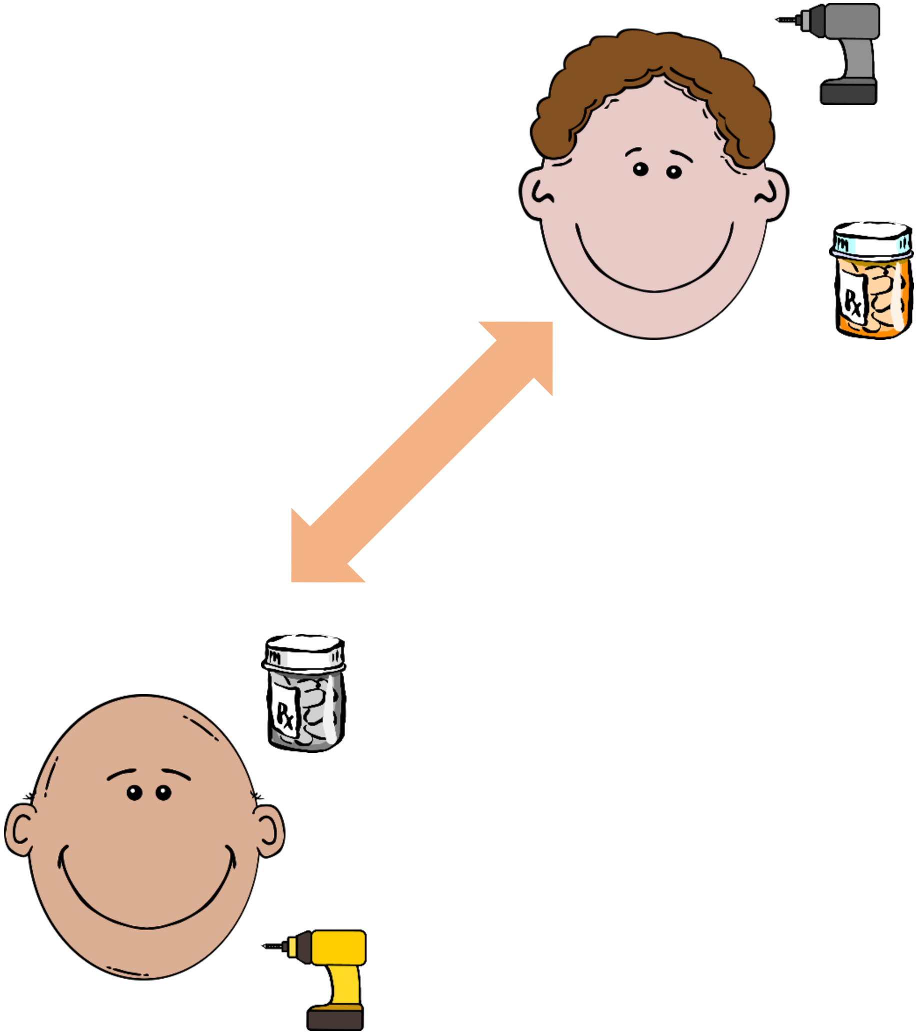
Traditional Currencies

1. Barter

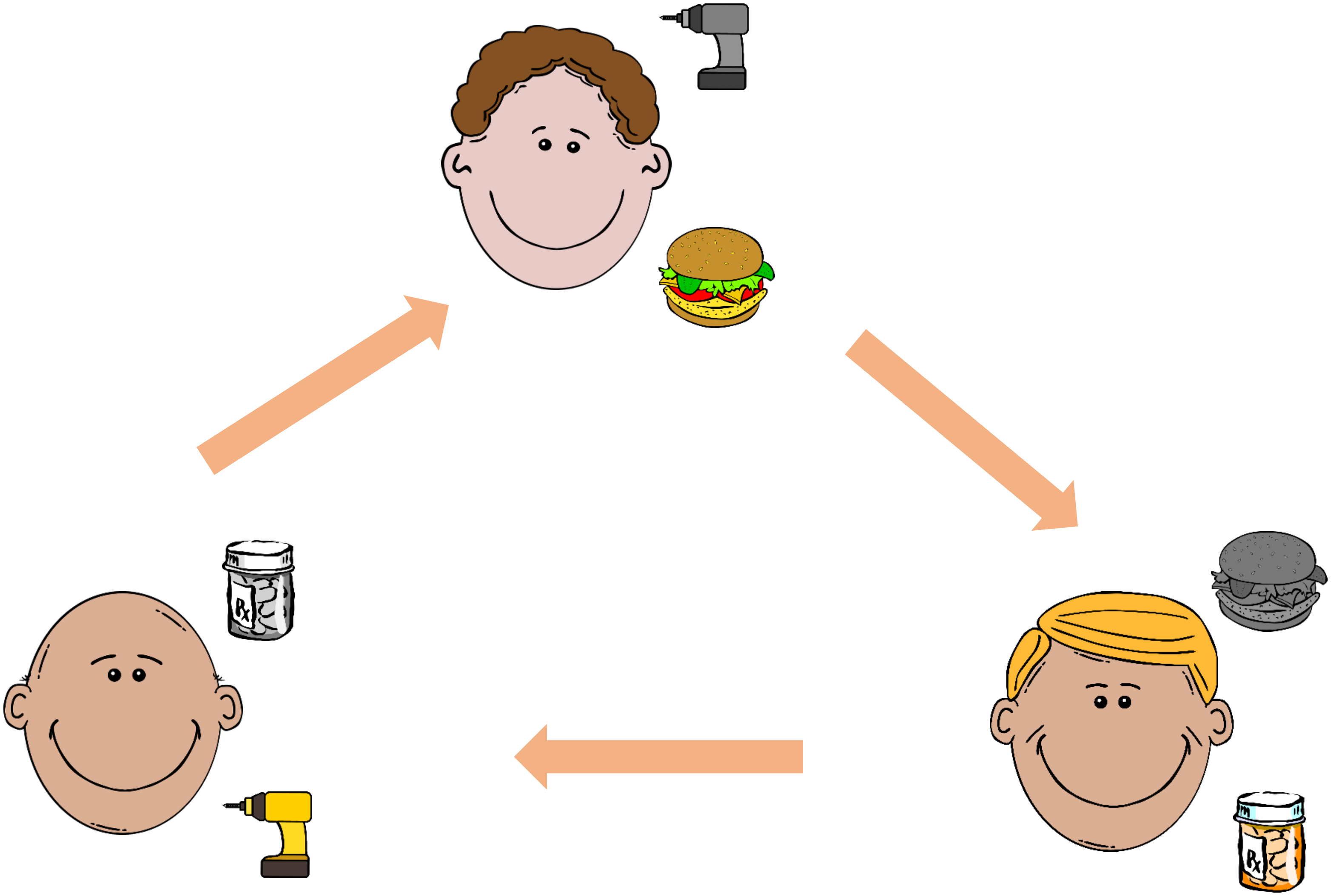
2. Credit

3. Cash

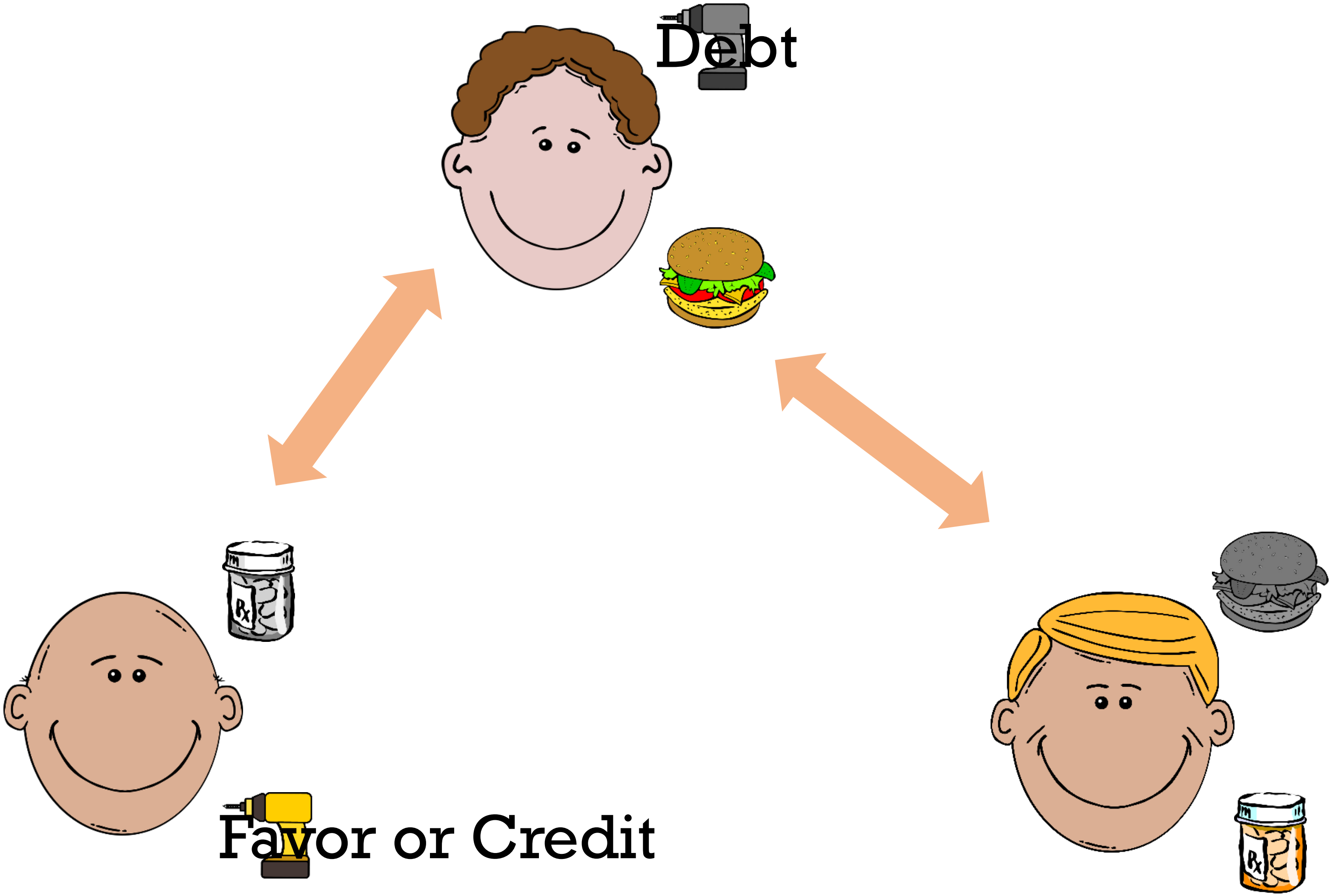
Barter



Barter



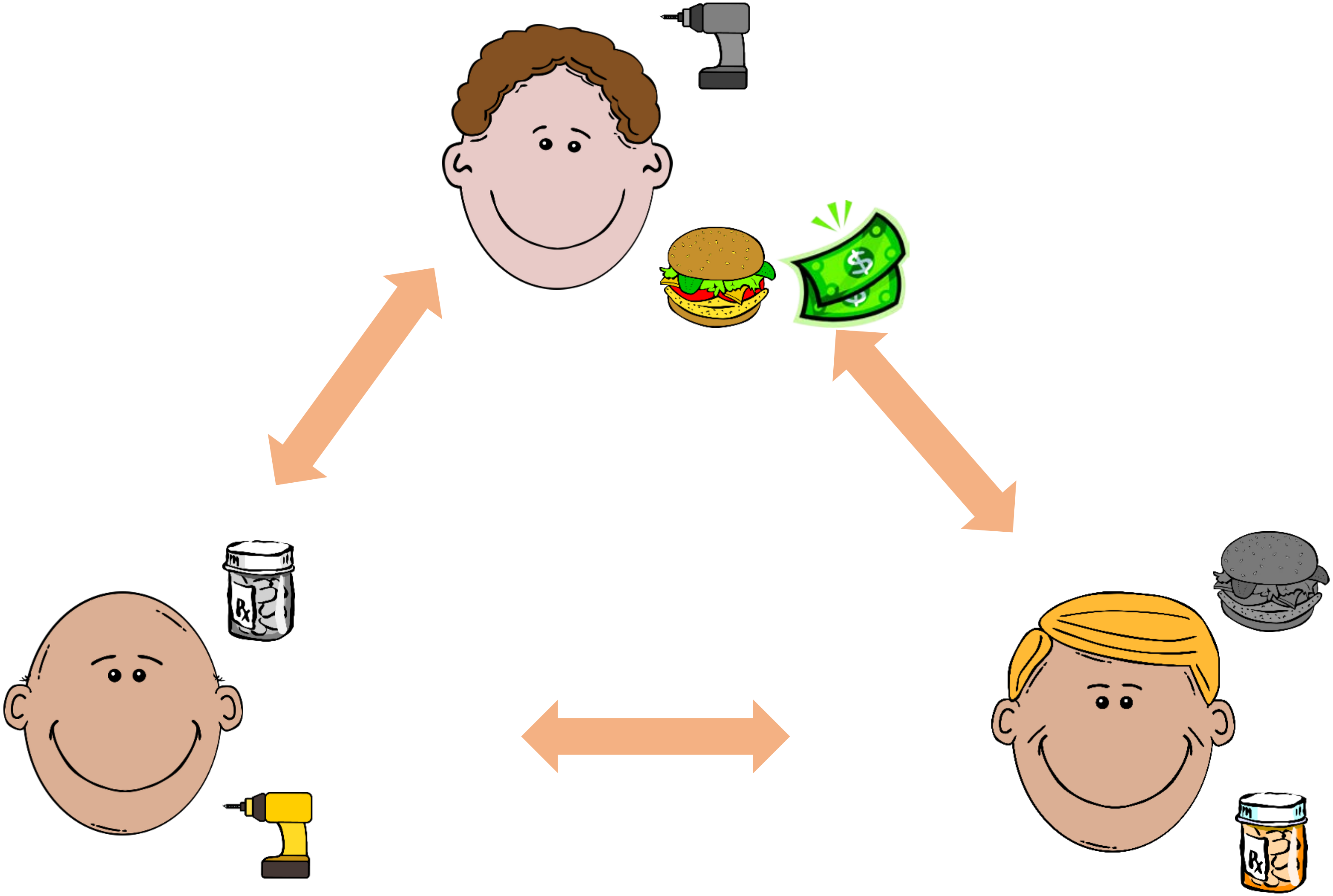
Credit



Debt

Favor or Credit

Cash

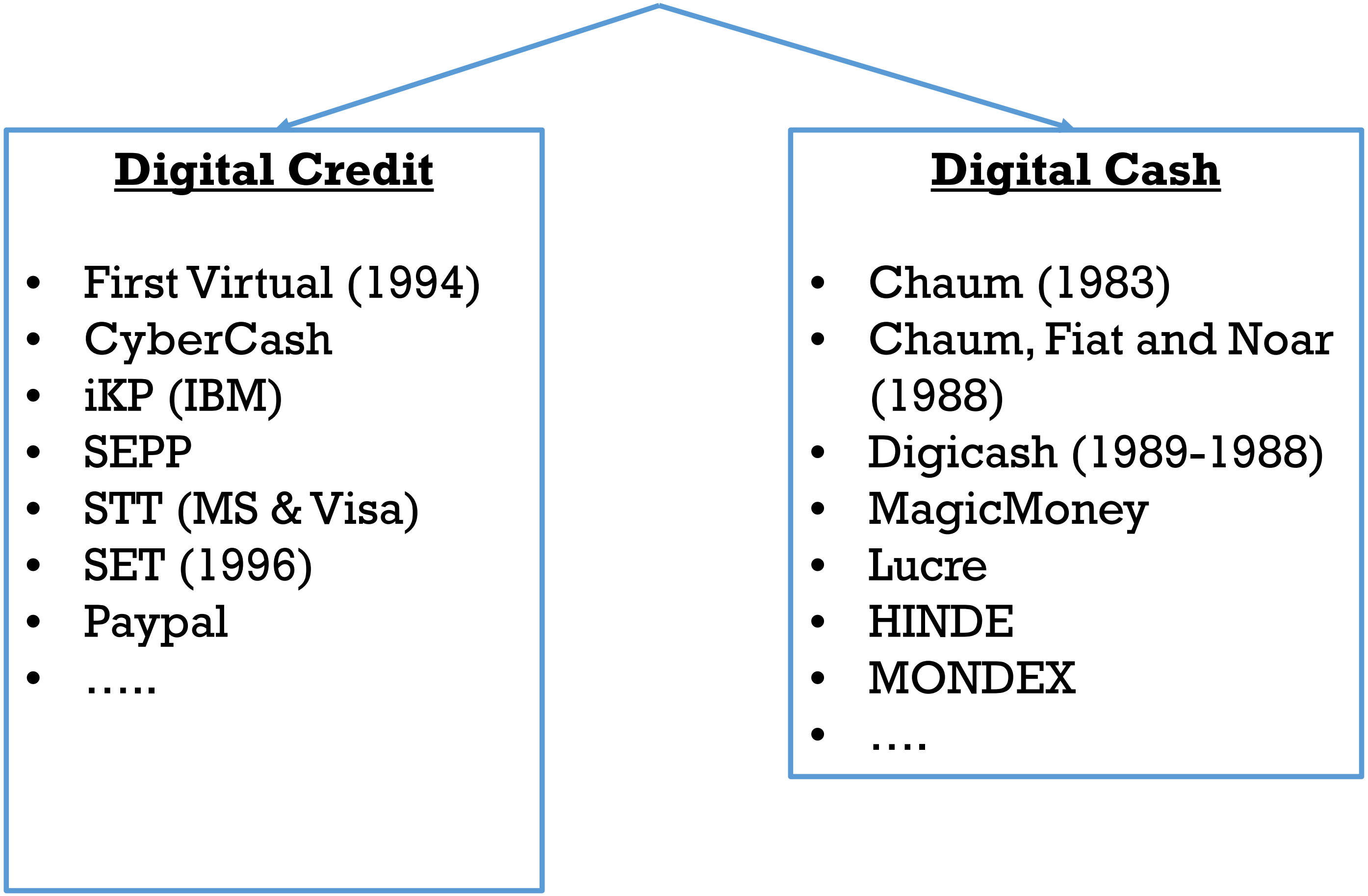


Cash vs Credit

- 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 Currency

Traditional Financial Tools for the Digital Realm



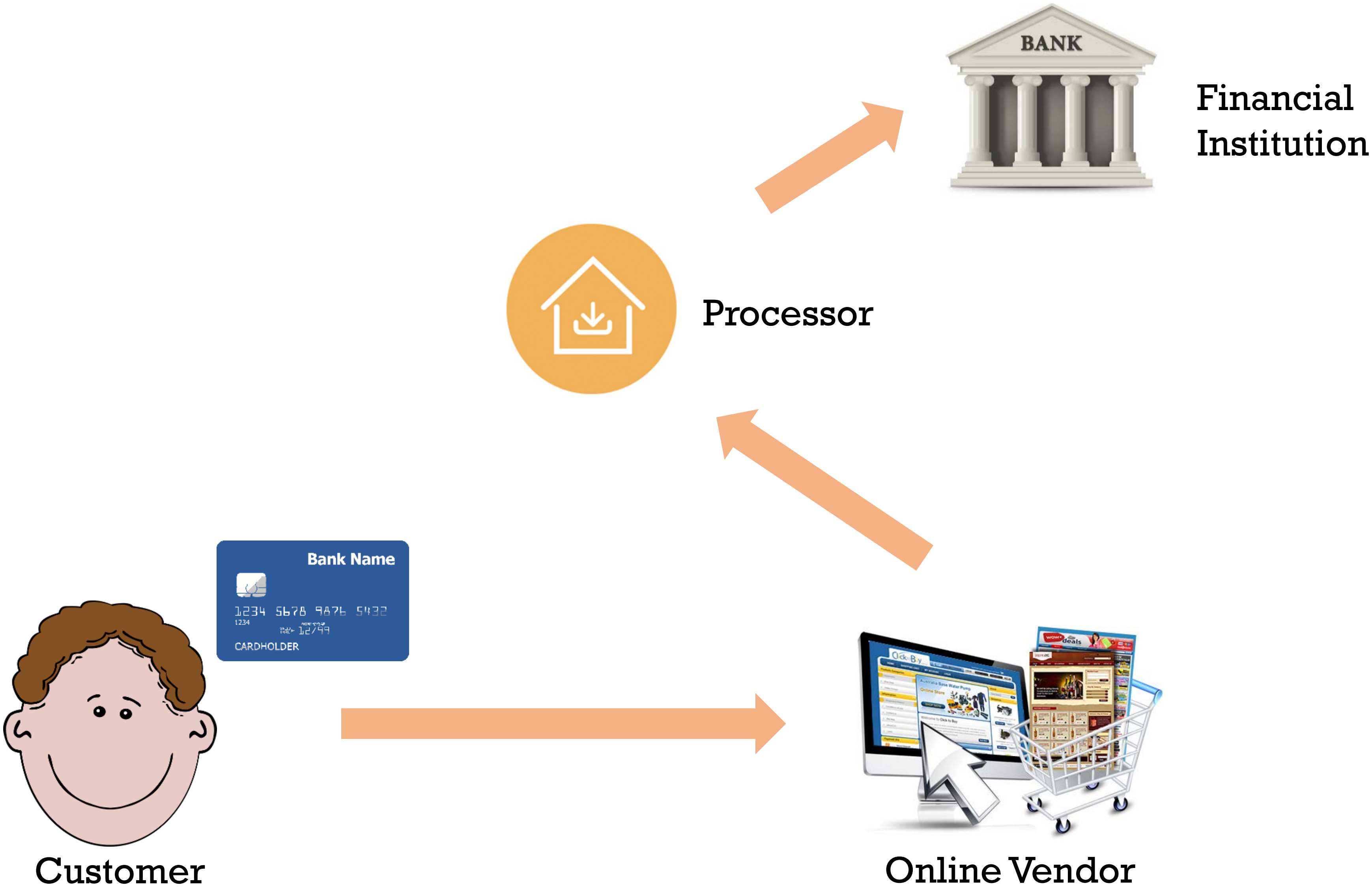
Digital Credit

- First Virtual (1994)
- CyberCash
- iKP (IBM)
- SEPP
- STT (MS & Visa)
- SET (1996)
- Paypal
- …..

Digital Cash

- Chaum (1983)
- Chaum, Fiat and Noar (1988)
- Digicash (1989-1988)
- MagicMoney
- Lucre
- HINDE
- MONDEX
- ….

Digital Credit Architecture 1



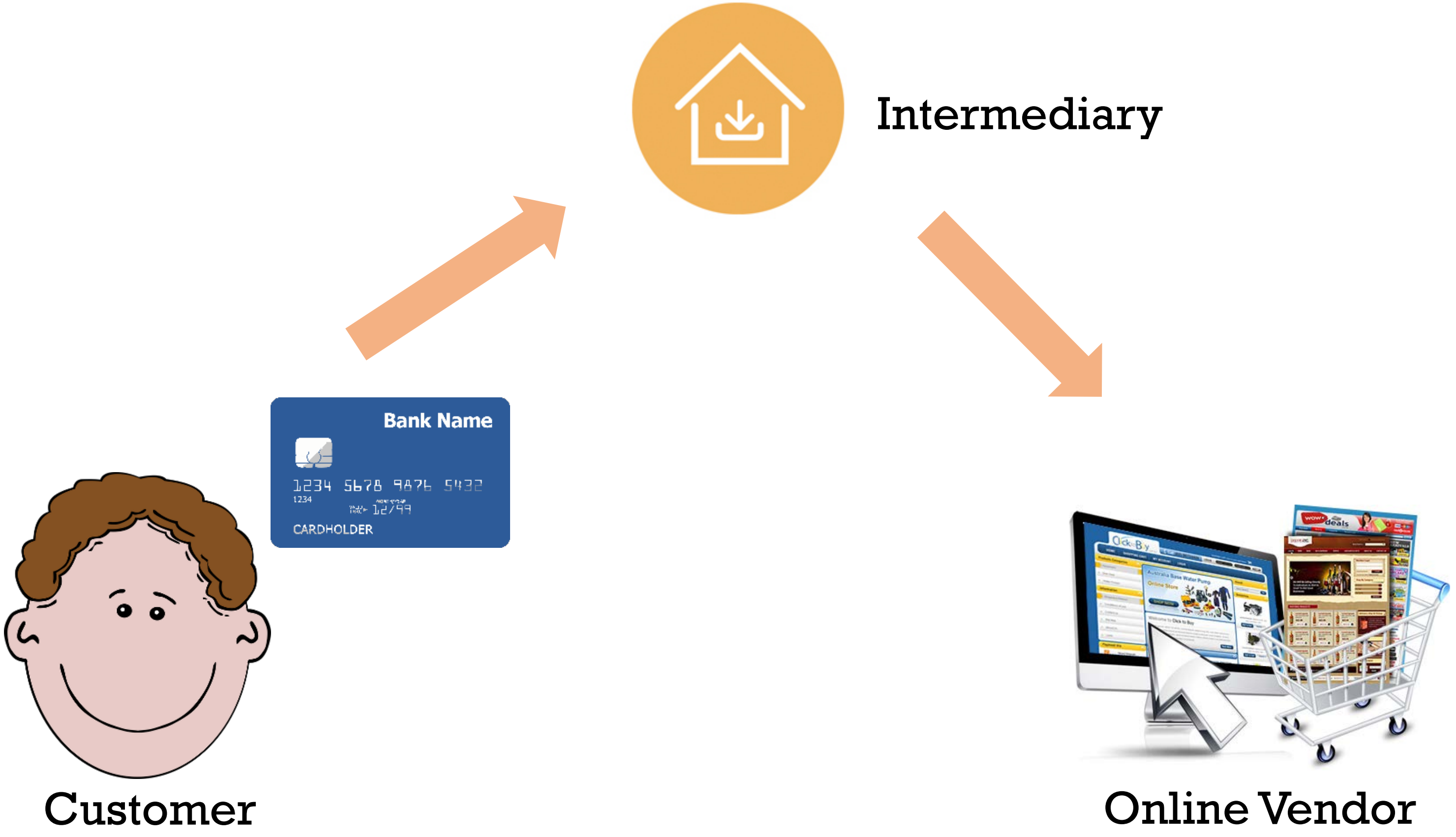
Financial Institution

Processor

Customer

Online Vendor

Digital Credit Architecture 2



Intermediary

Customer

Online Vendor

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

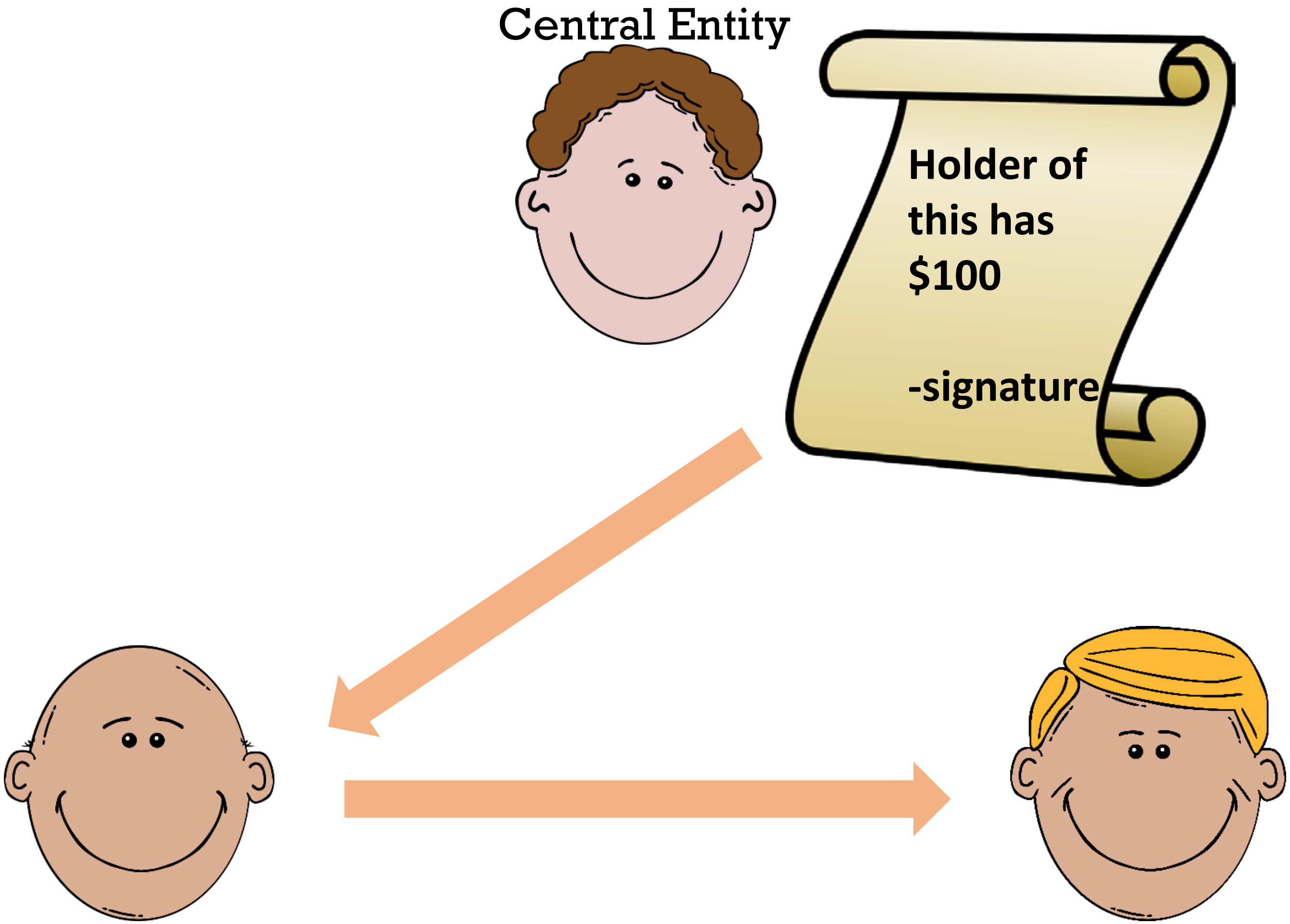
Digital Cash

- 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)



Central Entity

Holder of this has $100

-signature

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!

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!

Key Enabler

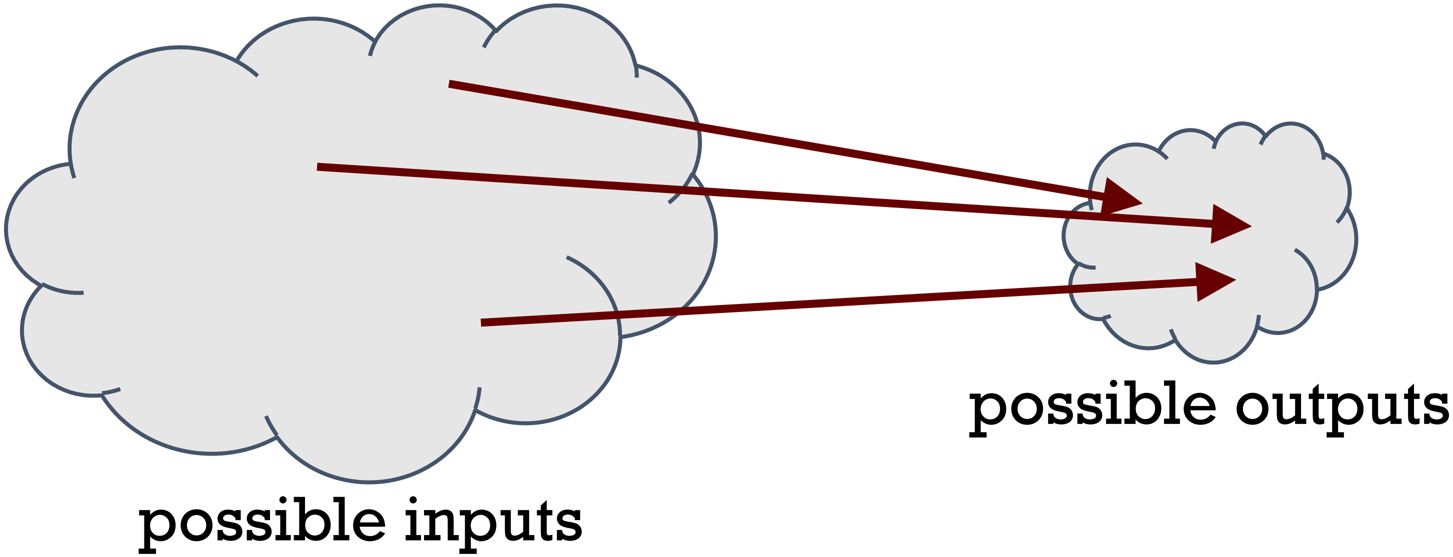
- How to create and maintain an append-only, immutable record or ledger of transactions
  - in a *distributed fashion* without requiring any centralized entity, and,
  - without requiring any *specialized hardware*, and,
  - without requiring *complex cryptography*, and,
  - such that it provides *user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

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

Talk Outline

- Crypto Background
- Bitcoin Details
- What’s Next

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* | *x*) ∈ *Y*.

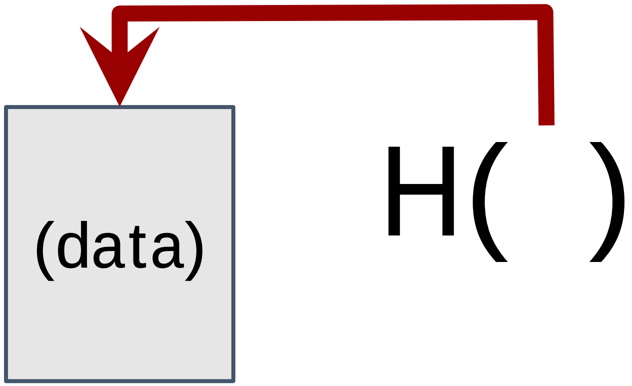
Puzzle-friendly property implies that no solving strategy is much better than trying random values of x.

Hash Pointers

- What is a Hash pointer?
  1. Pointer to where some info/data is stored, and
  2. (Cryptographic) hash of the info.

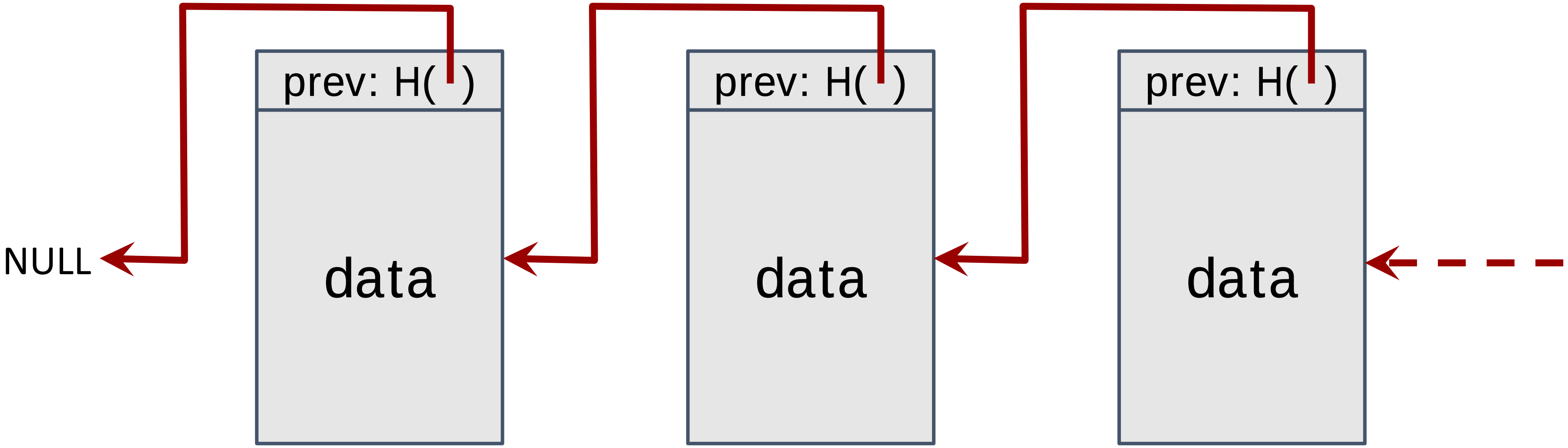
- What can you do with a hash pointer?
  - Retrieve or get back the info/data.
  - Verify that the info/data hasn't changed.
  - What else?

Use hash pointers to construct data structures such as blockchains!



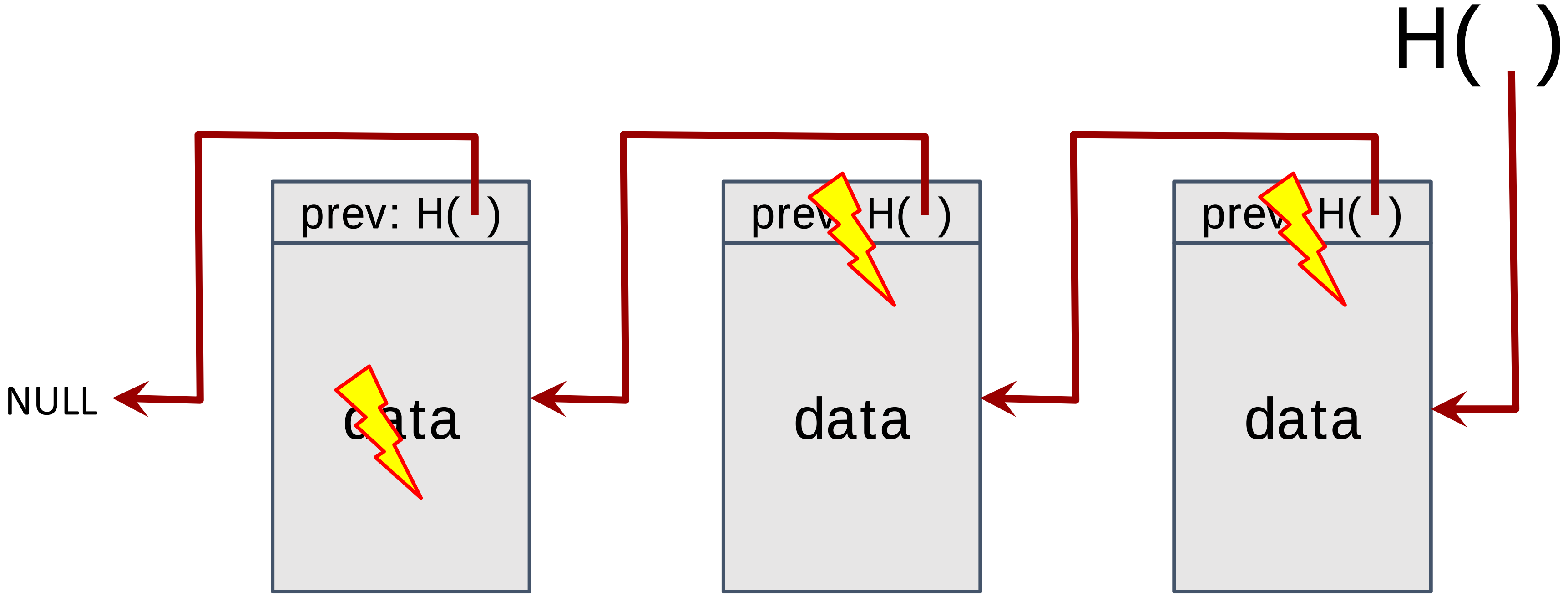
Blockchains

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



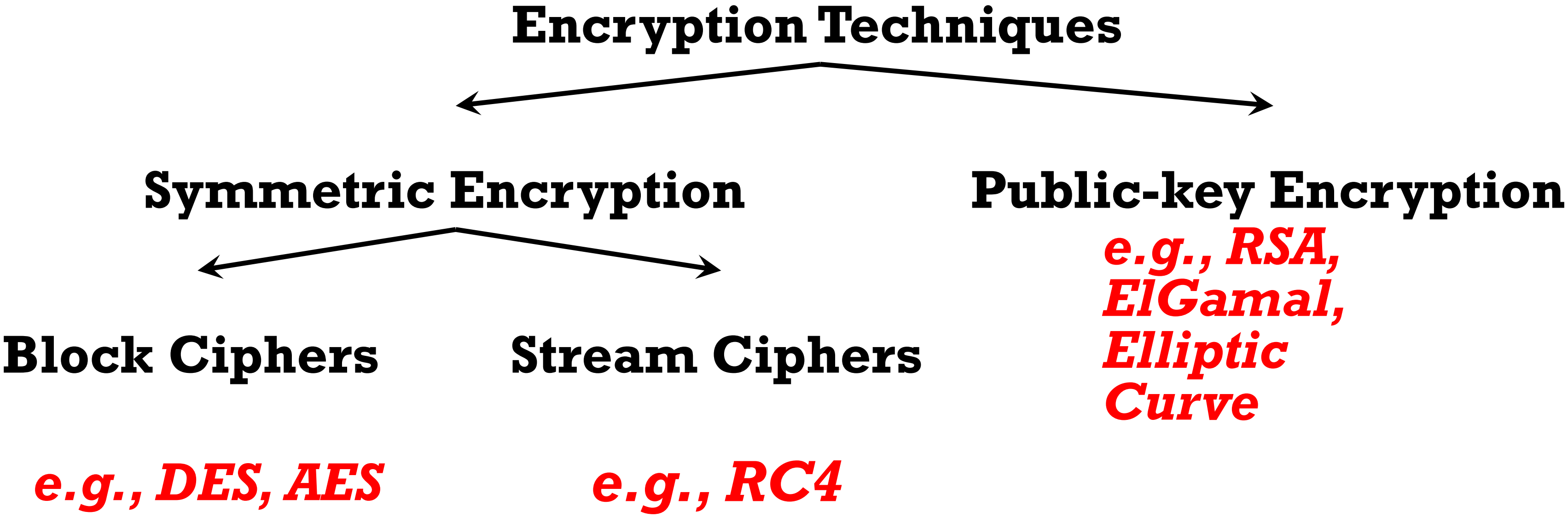
Head of the list (Genesis block)

Tamper-evident Log



Encryption

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



Encryption Techniques

Symmetric Encryption

Public-key Encryption

e.g., RSA, ElGamal, Elliptic Curve

Block Ciphers

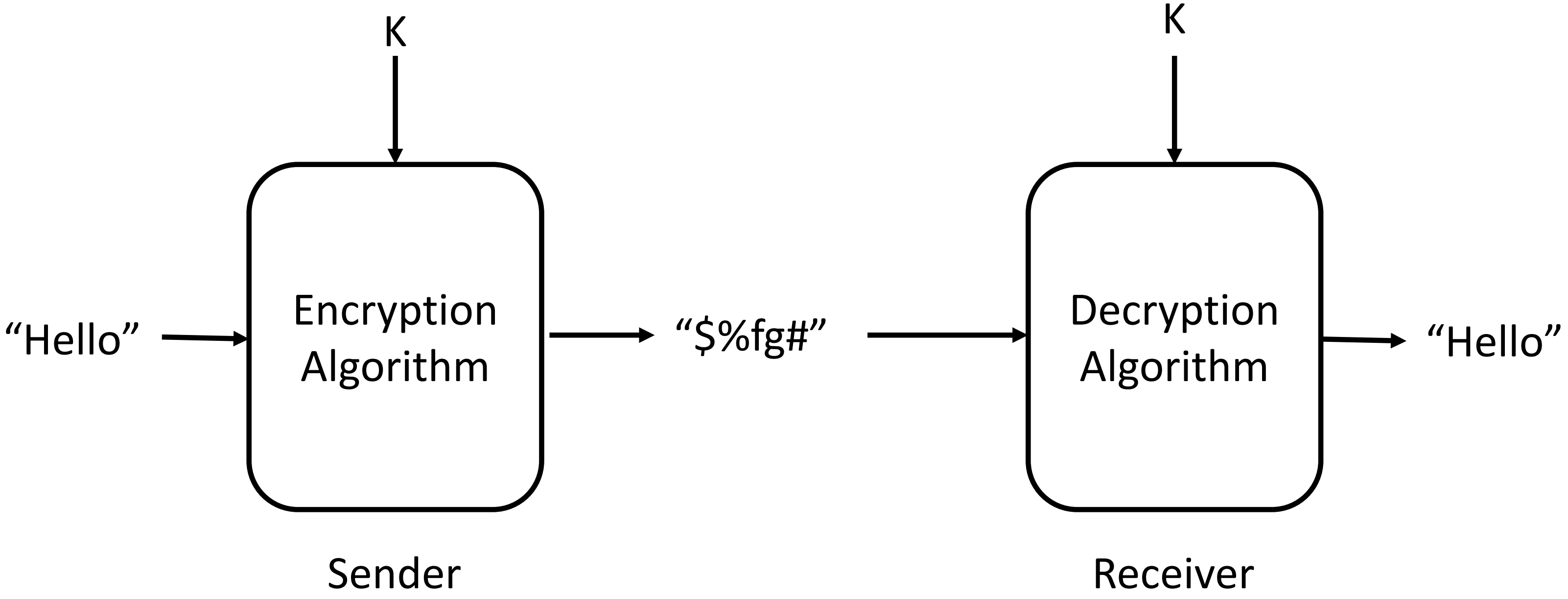
Stream Ciphers

e.g., DES, AES

e.g., RC4

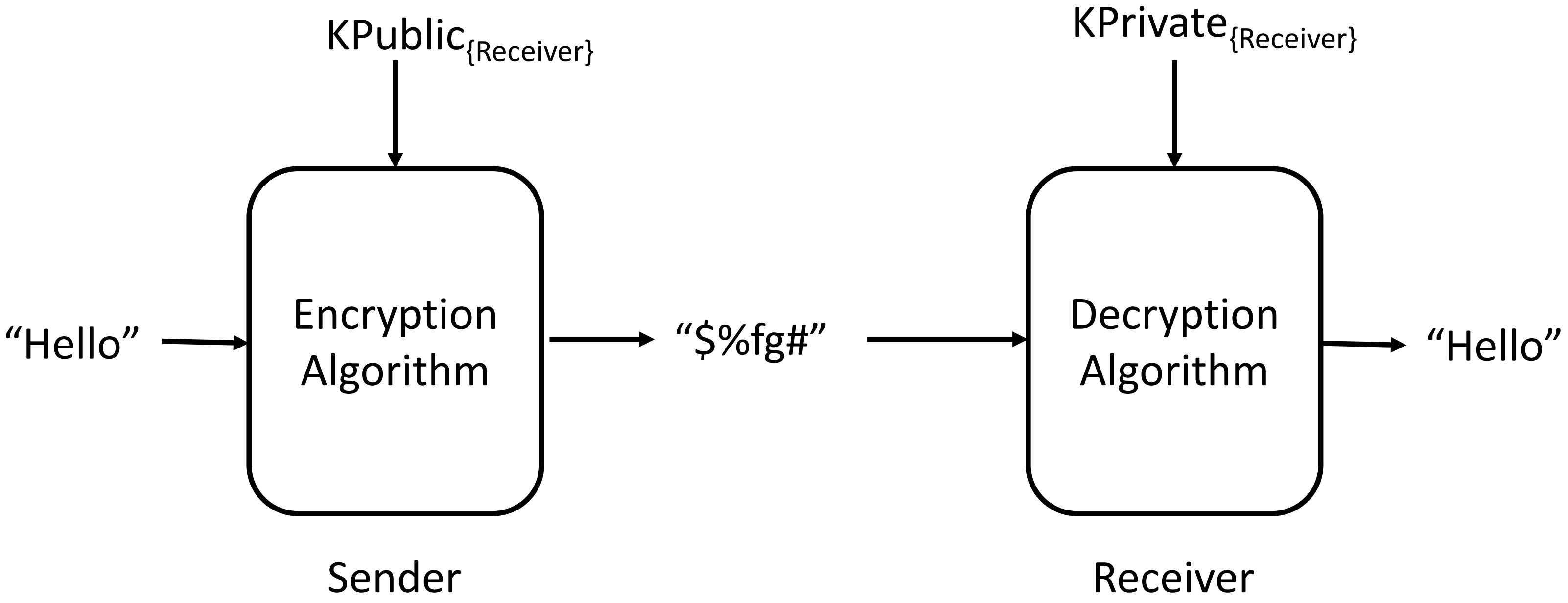
Symmetric Encryption

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

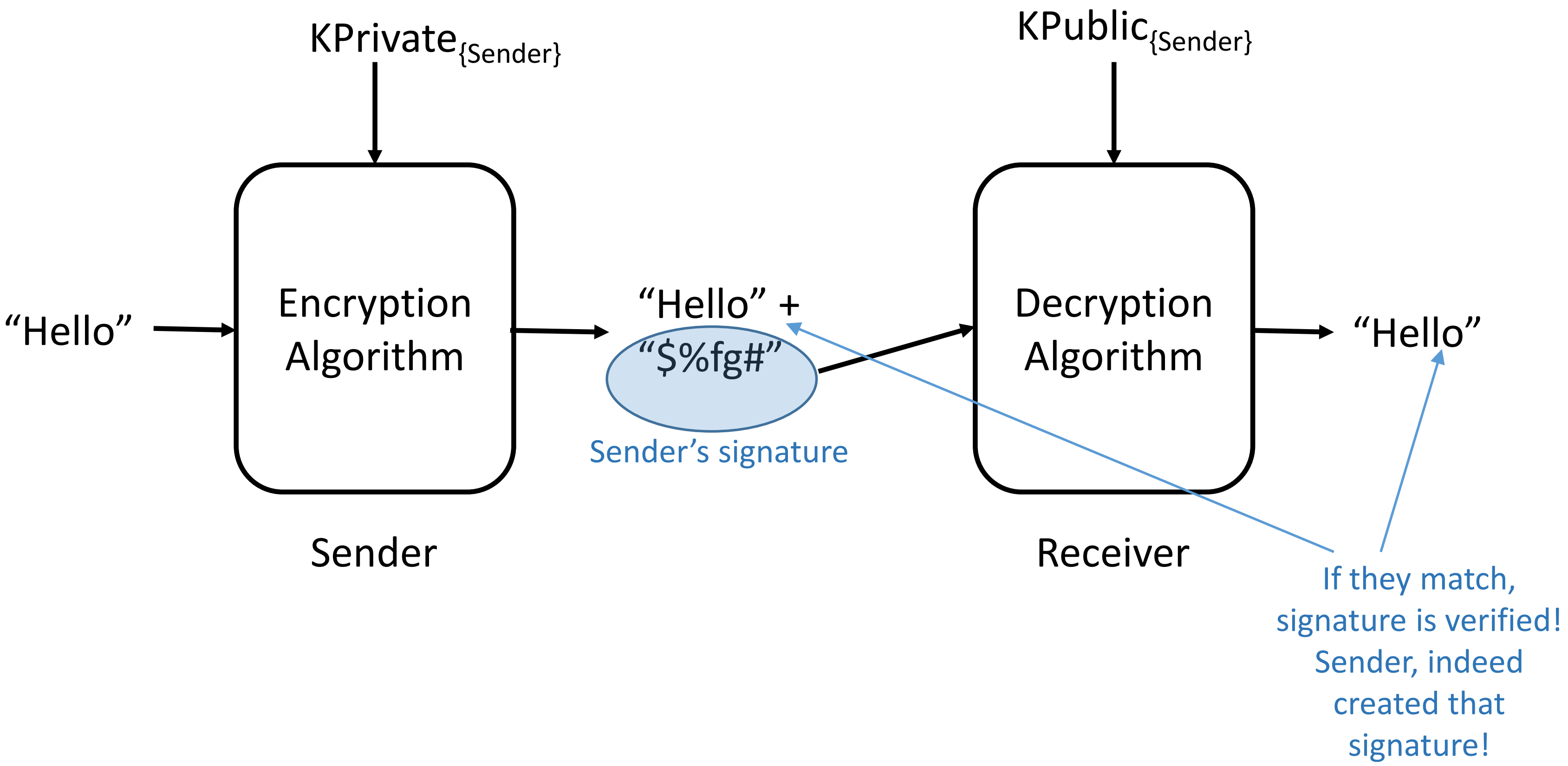


Public-Key Encryption

- **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.

Talk Outline

- Crypto Background
- Bitcoin Details
- What’s Next

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*?

A Bitcoin Transaction

metadata

```
{
        "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
        "ver":1,
        "vin_sz":2,
        "vout_sz":1,
        "lock_time":0,
        "size":404,
```

input(s)

```
        "in":[
          {
            "prev_out":{
              "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
              "n":0
            },
               "scriptSig":"30440..."
          },
          {
            "prev_out":{
              "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
              "n":0
            },
            "scriptSig":"3f3a4ce81...."
          }
        ],
```

output(s)

```
        "out":[
          {
            "value":"10.12287097",
            "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
          }
        ]
}
```

Transaction Metadata

```
                          {
transaction hash  {           "hash":"5a42590...b8b6b",
                  {             "ver":1,
housekeeping      {             "vin_sz":2,
                  {             "vout_sz":1,
"not valid before" {            "lock_time":0,
housekeeping      {             "size":404,
                           ...
                          }
```

also serves as a unique ID

Transaction Inputs

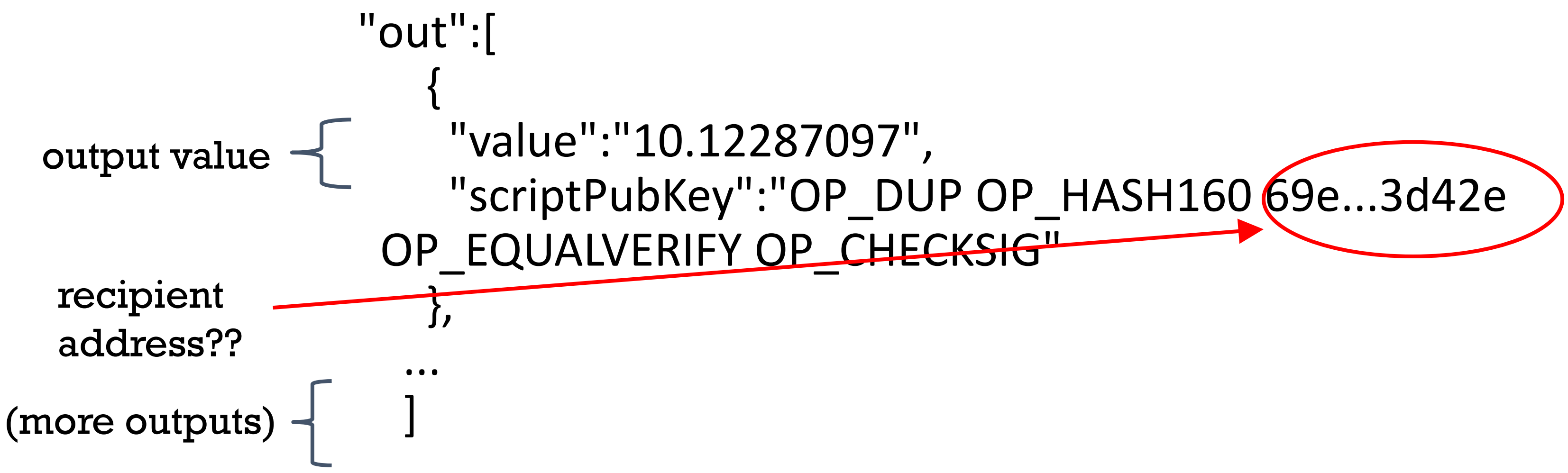
previous transaction

signature

(more inputs)

```
"in":[
    {
      "prev_out":{
        "hash":"3be4...80260",
        "n":0
      },
    "scriptSig":"30440....3f3a4ce81"
    },
  ...
],
```

Transaction Outputs



```
"out":[
   {
     "value":"10.12287097",
     "scriptPubKey":"OP_DUP OP_HASH160 69e...3d42e
 OP_EQUALVERIFY OP_CHECKSIG"
   },
  ...
  ]
```

output value

recipient address??

(more outputs)

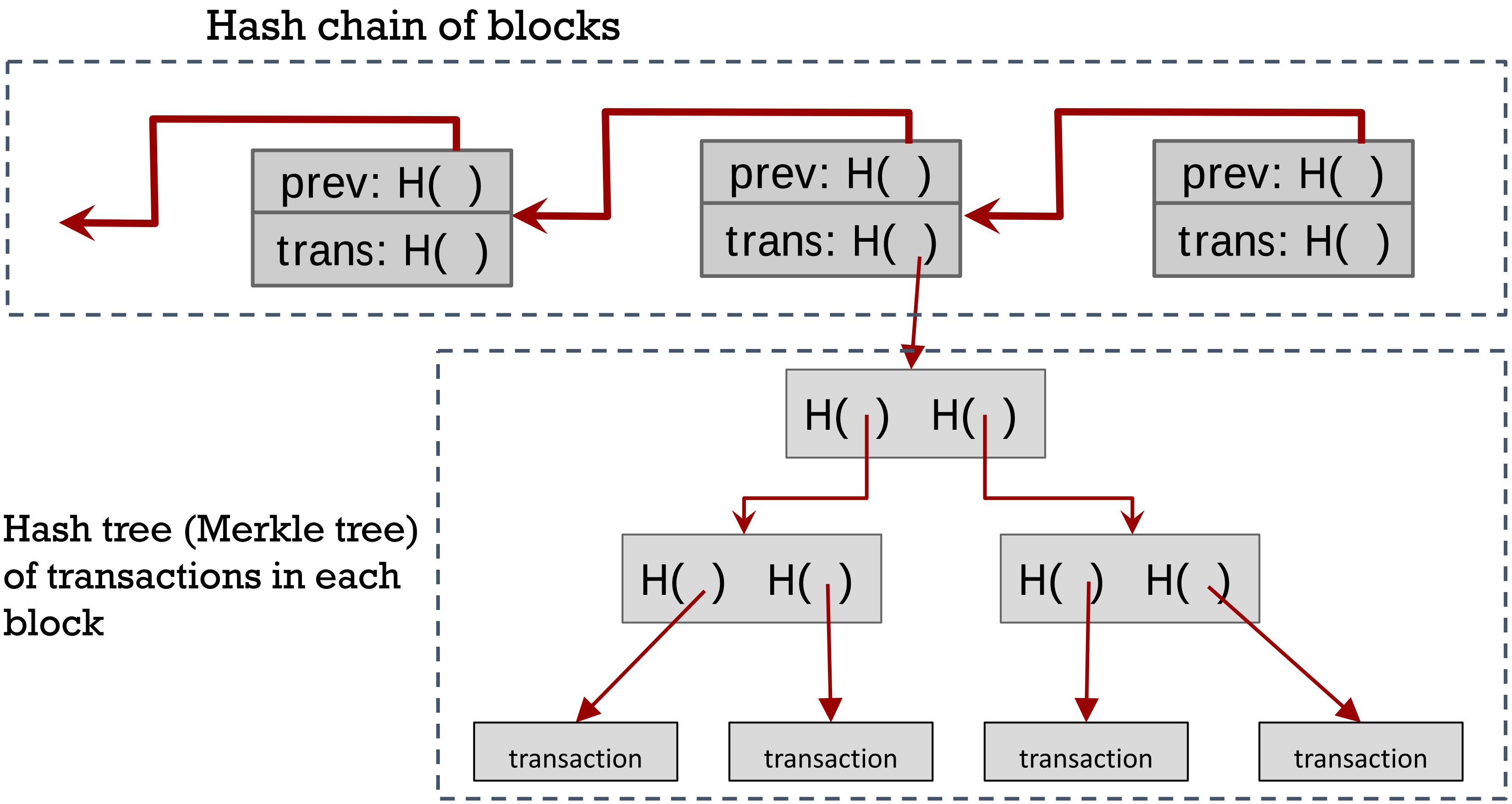
Sum of all output values less than or equal to sum of all input values!

If sum of all output values less than sum of all input values, then difference goes to miner as a transaction fee

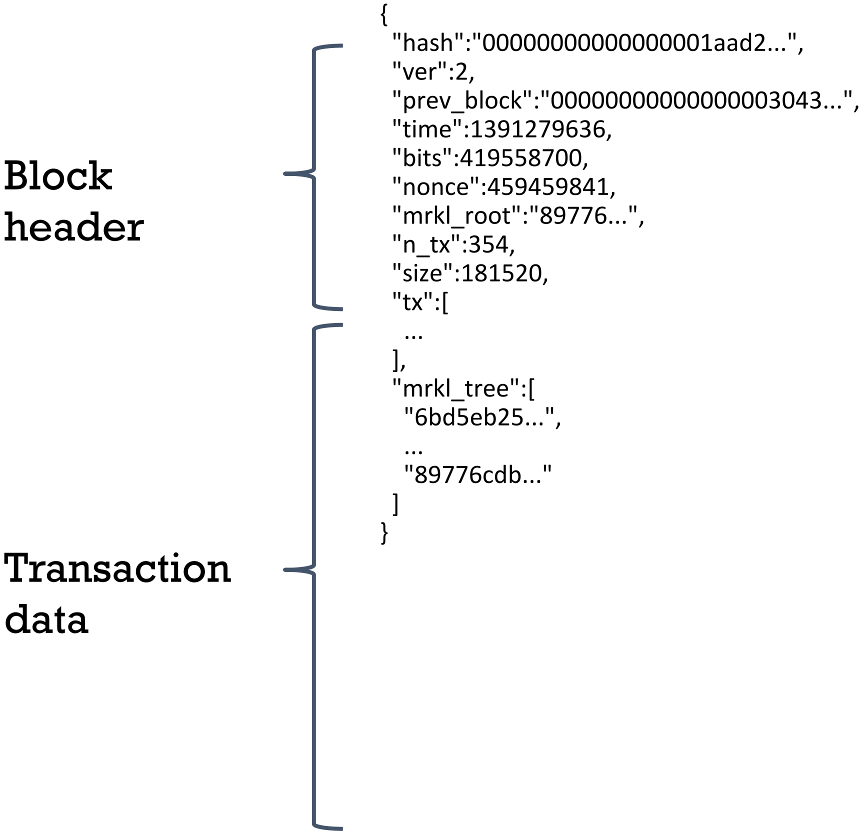
Bitcoin Blocks

- 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

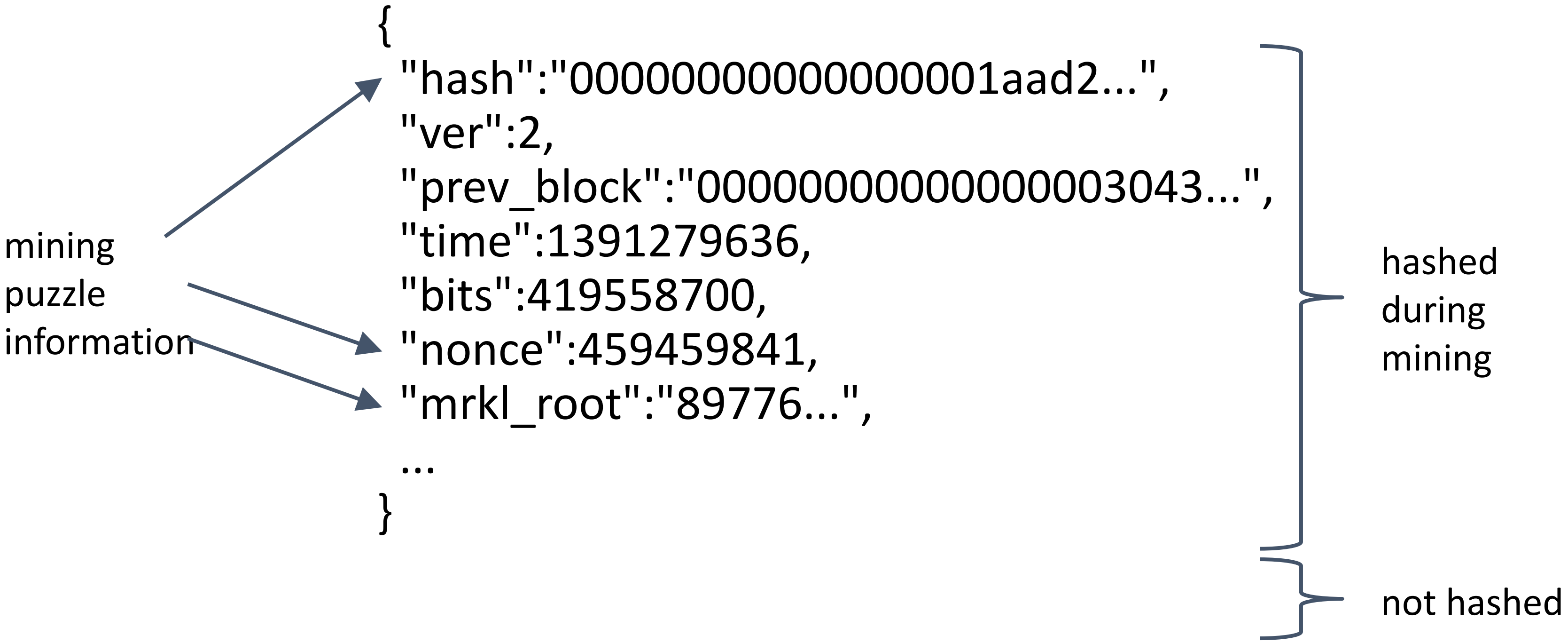


Block header

Transaction data

```
{
  "hash":"00000000000000001aad2...",
  "ver":2,
  "prev_block":"00000000000000003043...",
  "time":1391279636,
  "bits":419558700,
  "nonce":459459841,
  "mrkl_root":"89776...",
  "n_tx":354,
  "size":181520,
  "tx":[
    ...
  ],
  "mrkl_tree":[
    "6bd5eb25...",
    ...
    "89776cdb..."
  ]
}
```

A Bitcoin block header



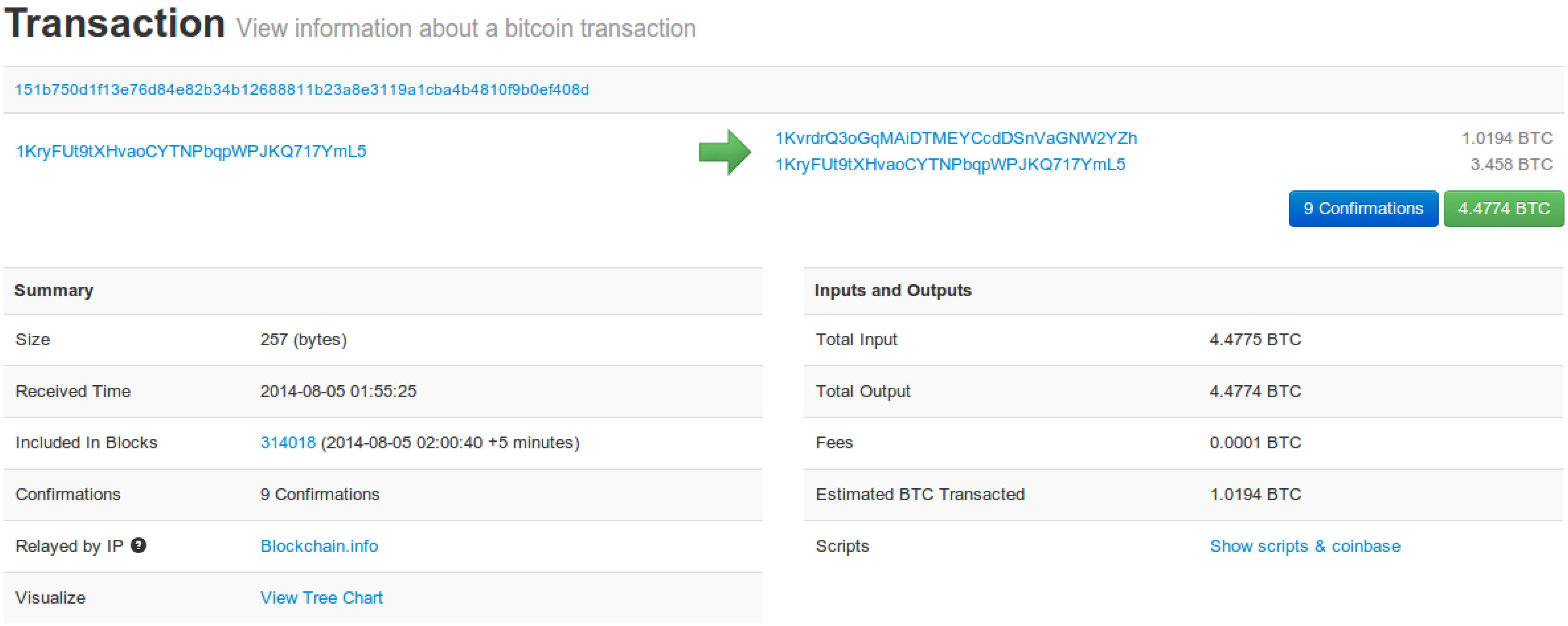
```
{
 "hash":"00000000000000001aad2...",
 "ver":2,
 "prev_block":"00000000000000003043...",
 "time":1391279636,
 "bits":419558700,
 "nonce":459459841,
 "mrkl_root":"89776...",
 ...
}
```

mining puzzle information

hashed during mining

not hashed

See for yourself!



Transaction View information about a bitcoin transaction

151b750d1f13e76d84e82b34b12688811b23a8e3119a1cba4b4810f9b0ef408d

1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5	→	1KvrdrQ3oGqMAiDTMEYCcdDSnVaGNW2YZh	1.0194 BTC
		1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5	3.458 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 (and many other sites)

Bitcoin Summary

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

- Three Important Aspects of Bitcoins :
    - Data structures.
    - Bitcoin peer-to-peer network.
    - Consensus.

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

More on this later!

- 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!

Bitcoin Summary

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

- Three Important Aspects of Bitcoins
  - Data structures.
  - Bitcoin peer-to-peer network.
  - Consensus.

Bitcoin Consensus

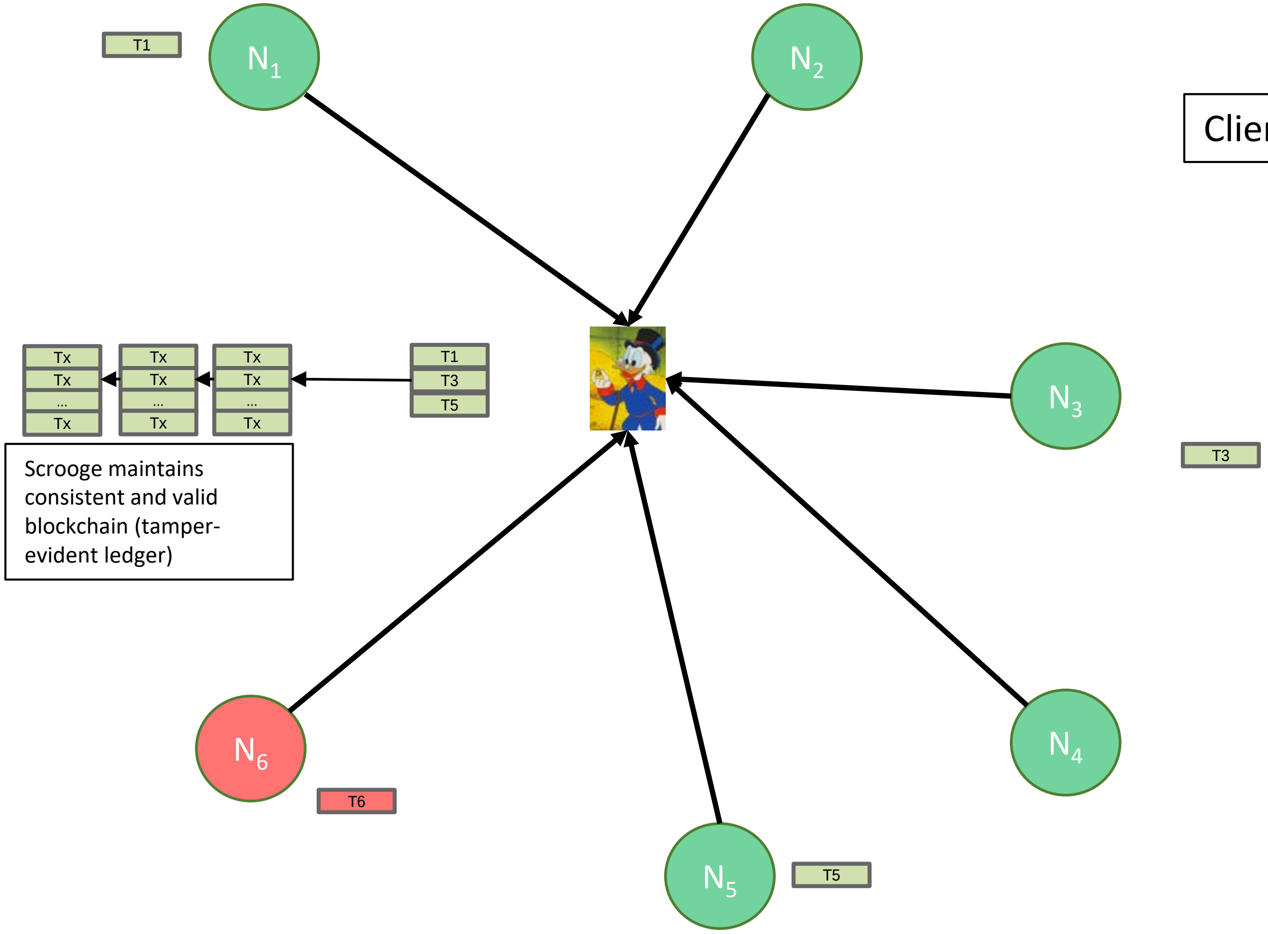
- Bitcoin Consensus – most important functionality of the Bitcoin P2P network.

- What do Bitcoin nodes need to reach a consensus on?
    - Which <u>transactions</u> were broadcast on the network.
    - <u>Order</u> in which these transactions occurred.
    - Transactions are valid (output<=input and not double spent).

→ Result of the consensus protocol: Consistent, valid and immutable global transaction ledger.

How Centralized Consensus Works

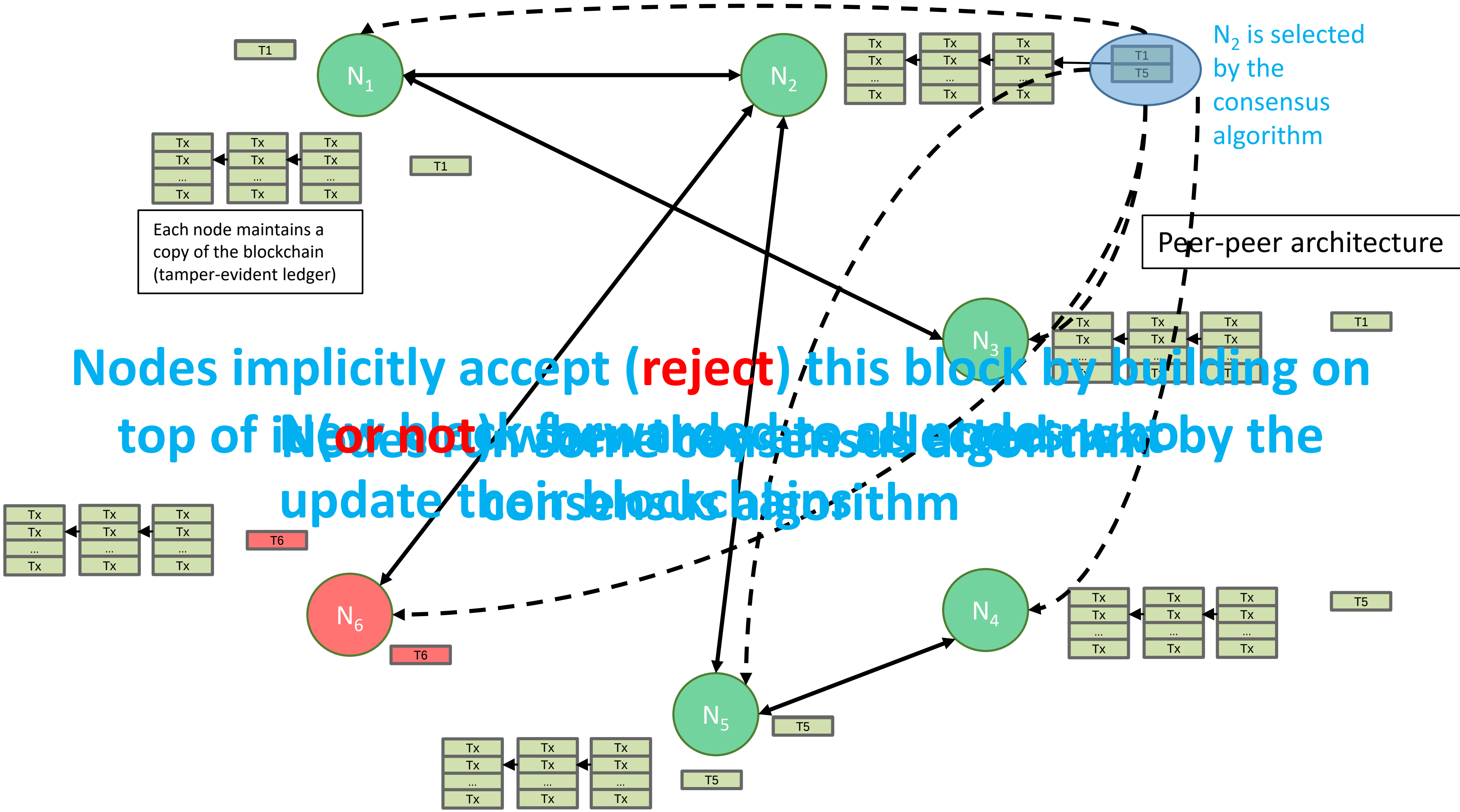
Client-server architecture



Scrooge maintains consistent and valid blockchain (tamper-evident ledger)

🟢 Honest nodes/users 🔴 Malicious nodes/users

How Bitcoin Consensus Works



N2 is selected by the consensus algorithm

Each node maintains a copy of the blockchain (tamper-evident ledger)

Peer-peer architecture

Nodes implicitly accept (reject) this block by building on top of it (or not) when they are selected by the consensus algorithm

New block forwarded to all nodes who update their blockchains

Nodes run some consensus algorithm

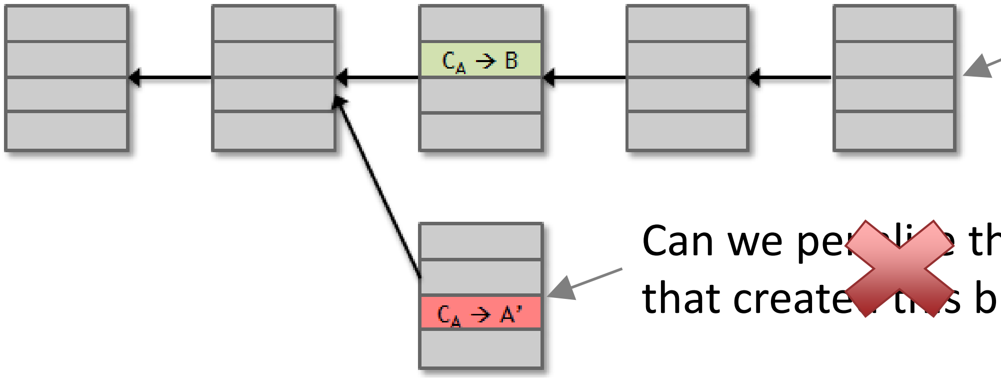
Why consensus in Bitcoin is hard?

1. Nodes may crash or become offline.
2. Peer-to-peer network is imperfect.
   - Not all pairs of nodes connected (and may participate).
   - Faults in network.
   - Latency.

No notion of global time → constraints the set of consensus algorithms that can be used

3. Nodes may be malicious.

Assumption of Honesty is Problematic



Can we reward nodes that created these blocks?

Can we penalize the node that created this block?

In other words, can we give nodes incentives for behaving honestly?

✓ We can utilize the fact that Bitcoin (the currency) has value to achieve distributed consensus!

Incentive 1: Block Reward

Creator of block gets to

- include special coin-creation transaction in the block.
- choose recipient address of this transaction.

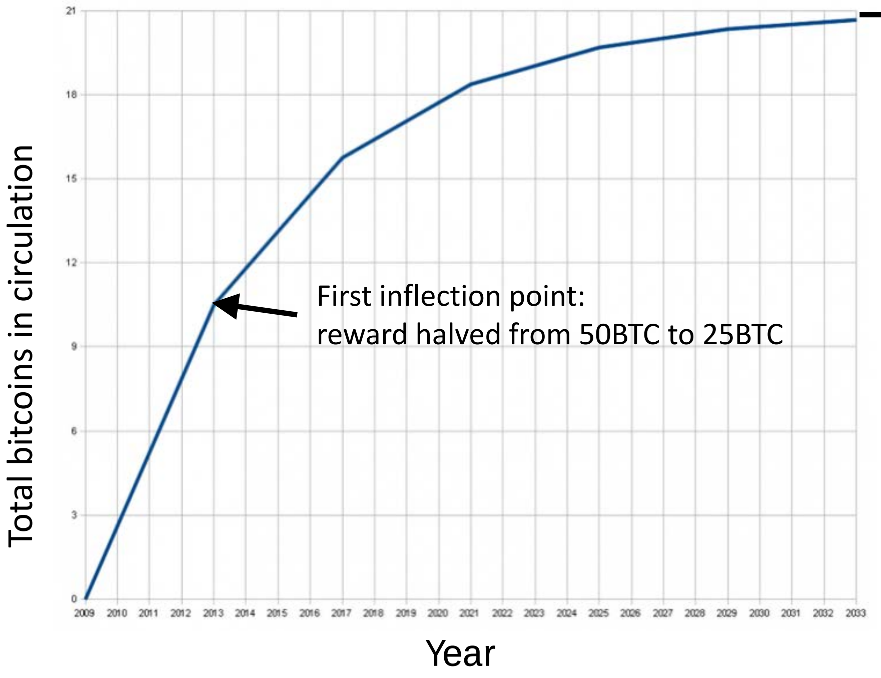
Value is fixed: currently 12.5 BTC, halves every 210,000 blocks created (or every 4 years at the current rate of block creation).

- We are now in the third period – first period block reward was 50 BTC.
- Reward drops to 6.25 BTC on 24th May 2020, 16:11:39 (est).

Block creator gets to "collect" the reward only if the block ends up on long-term consensus branch!

- Subtle but powerful trick: Incentivizes nodes to behave in way that will get other nodes to extend their block.

There’s a finite supply of bitcoins



First inflection point:
reward halved from 50BTC to 25BTC

Total supply: 21 million

Block reward is how
new bitcoins are created

Runs out in 2040. No new
bitcoins unless rules change

Does that mean that after 2040, nodes will no longer have incentive to behave honestly?

Not really!

Incentive 2: Transaction Fees

- Creator of transaction can choose to make output value less than input value.

- Remainder is a transaction fee and goes to block creator.

- Purely voluntary, like a tip.
  - But system will evolve, and will become mandatory, as Block rewards run out.

A Coinbase Transaction

```
"in":[
    {
      "prev_out":{
        "hash":"000000.....0000000",
        "n":4294967295
      },
    "coinbase":"..."
    },
   "out":[
 {
  "value":"12.53371419",
  "scriptPubKey":"OPDUP OPHASH160 ... ”
   }
```

redeeming nothing

arbitrary

Null hash pointer

First ever coinbase parameter:
“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

block reward

transaction fees

Remaining Problems

1. How to pick a random node?

2. How to avoid a free-for-all system due to rewards?
   - Everybody may want to run a bitcoin node in order to get free rewards.

3. How to prevent Sybil attacks?
   - An adversary may create a large number of Sybil nodes to subvert the consensus process.

Solution: Mining using Proof-of-Work (PoW).

Proof of Work (PoW)

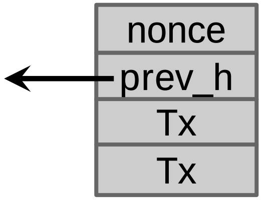
To approximate selecting a random node: *select nodes in proportion to a resource that no one can monopolize (we hope):*

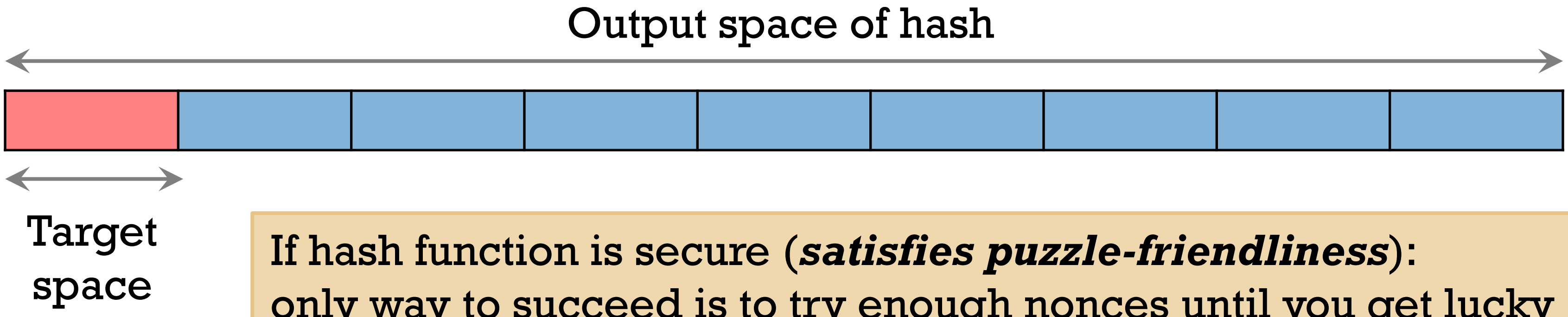
- In proportion to computing power: **proof-of-work** *(Used in Bitcoins).*
- In proportion to ownership of the currency: **proof-of-stake** (*Not used in Bitcoins – but a legitimate model used in other cryptocurrencies*).

Hash Puzzles

To create block, find nonce s.t.
H(nonce ‖ prev_hash ‖ tx ‖ … ‖ tx) is very small.

In other words, *H(nonce ‖ prev_hash ‖ tx ‖ … ‖ tx) < target .*





If hash function is secure (***satisfies puzzle-friendliness***):
only way to succeed is to try enough nonces until you get lucky

Mining Bitcoins in 6 Easy Steps

1. Join the network, listen for transactions.
   a. Validate all proposed transactions.
2. Listen for new blocks, maintain blockchain.
   a. When a new block is proposed, validate it.
3. Assemble a new valid block.
4. Find the nonce to make your block valid.
5. Hope everybody accepts your new block.
6. Profit!

Useful to Bitcoin network

Incentivize miners to do above

Advantage of a PoW System?

- It completely does away with the problem of magically picking a random node (to propose a block).

- Nodes independently compete by attempting to solve hash puzzles.
  - Once in a while, one (randomly) will succeed and propose the next block.
  - Result: Completely decentralized system → No one gets to decide which node proposes the next block.

- Other advantages:
  - Not a free-for-all system → Nodes need to work to get paid.
  - Creating new (Sybil) identities is useless without creating new computing power (to solve PoW) to go along with it!

Evolution of Mining

2009 → **2018**

CPU

GPU

FPGA

ASIC

Gold pan

Sluice box

Placer mining

Pit mining

How to Transact in Bitcoin?

To spend a Bitcoin, you need to know:

- Some info from the public blockchain, and
- The owner's secret signing key

So it's all about key management.

Goals as a Currency

1. **Availability**: Being able to spend your coins when you want to.

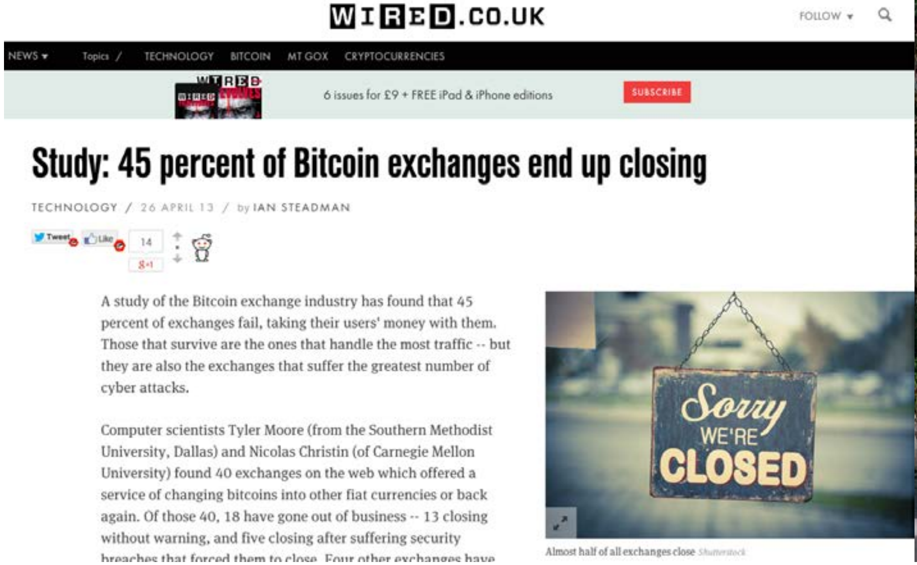
2. **Security**: Making sure nobody else can spend your coins.

3. **Convenience:** Managing your keys (and thus your coins)

Achieving all the three simultaneously could be a challenge!

Bitcoin Transaction Tools

1. Personally manage your keys.
2. Local wallet software.
3. Online wallet software.
4. Bank-like services or Bitcoin exchanges.



Study: 45 percent of Bitcoin exchanges end up closing

TECHNOLOGY / 26 APRIL 13 / by IAN STEADMAN

A study of the Bitcoin exchange industry has found that 45 percent of exchanges fail, taking their users' money with them. Those that survive are the ones that handle the most traffic -- but they are also the exchanges that suffer the greatest number of cyber attacks.

Computer scientists Tyler Moore (from the Southern Methodist University, Dallas) and Nicolas Christin (of Carnegie Mellon University) found 40 exchanges on the web which offered a service of changing bitcoins into other fiat currencies or back again. Of those 40, 18 have gone out of business -- 13 closing without warning, and five closing after suffering security breaches that forced them to close. Four other exchanges have

Almost half of all exchanges close Shutterstock

Anonymity

Anonymity = pseudonymity + **unlinkability**

Different interactions of the same user with the system should not be linkable to each other (and to the user's real identity)

Defining Unlinkability in Bitcoin

1. Hard to link together different addresses of the same user

2. Hard to link together different transactions made by the same user

3. Hard to link sender of a payment to its recipient

Why Anonymous Cryptocurrencies?

Blockchain based currencies are totally, publicly, and permanently traceable.

Without anonymity, privacy is much worse than traditional banking!

Two motivations:

1. Achieve privacy level at least equivalent to traditional banking
2. If possible, go beyond the privacy level offered by traditional banking based solutions

Ethical Concerns of Anonymity

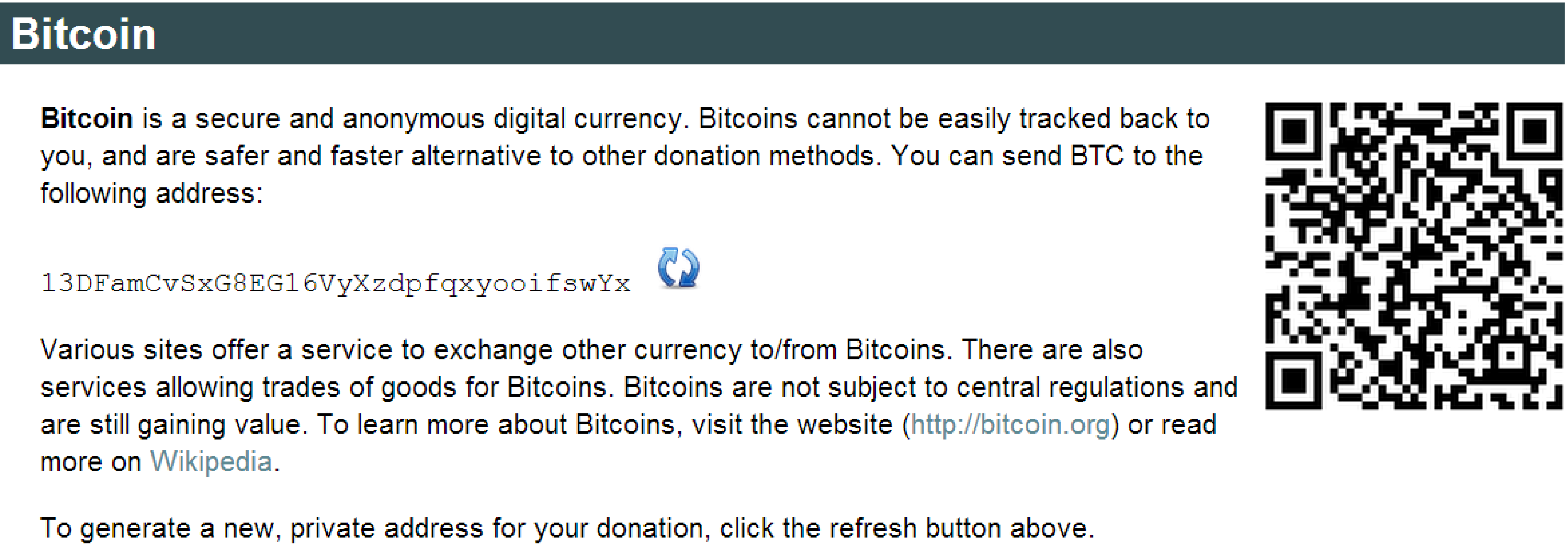
Legitimate “goods”: May prevent learning of sensitive information (e.g., someone’s salary).

Legitimate “worries” : Money laundering

Conundrum: Can we keep only the good uses?

Uses that are very different morally are pretty much the same technologically!

How to de-anonymize Bitcoin?



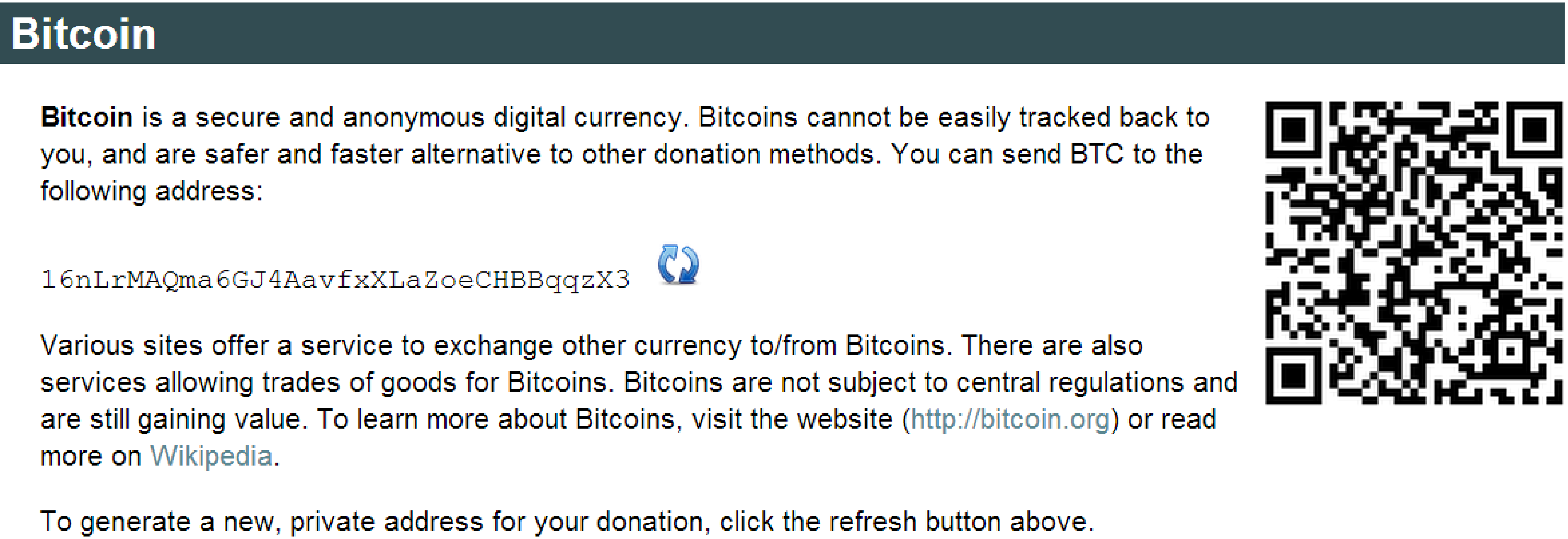
Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

```
13DFamCvSxG8EG16VyXzdpfqxyooifswYx
```

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

To generate a new, private address for your donation, click the refresh button above.



Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

`16nLrMAQma6GJ4AavfxXLaZoeCHBBqqzX3`

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

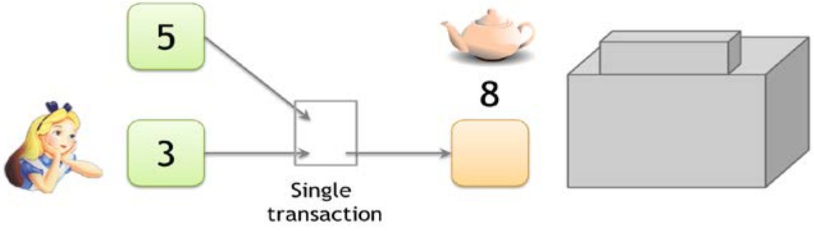
To generate a new, private address for your donation, click the refresh button above.

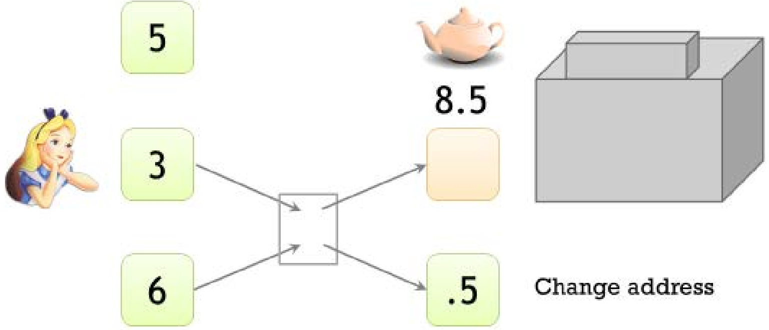
Trivial to create new address

Best practice: Always receive at fresh address.

So, unlinkable?

Linking Addresses



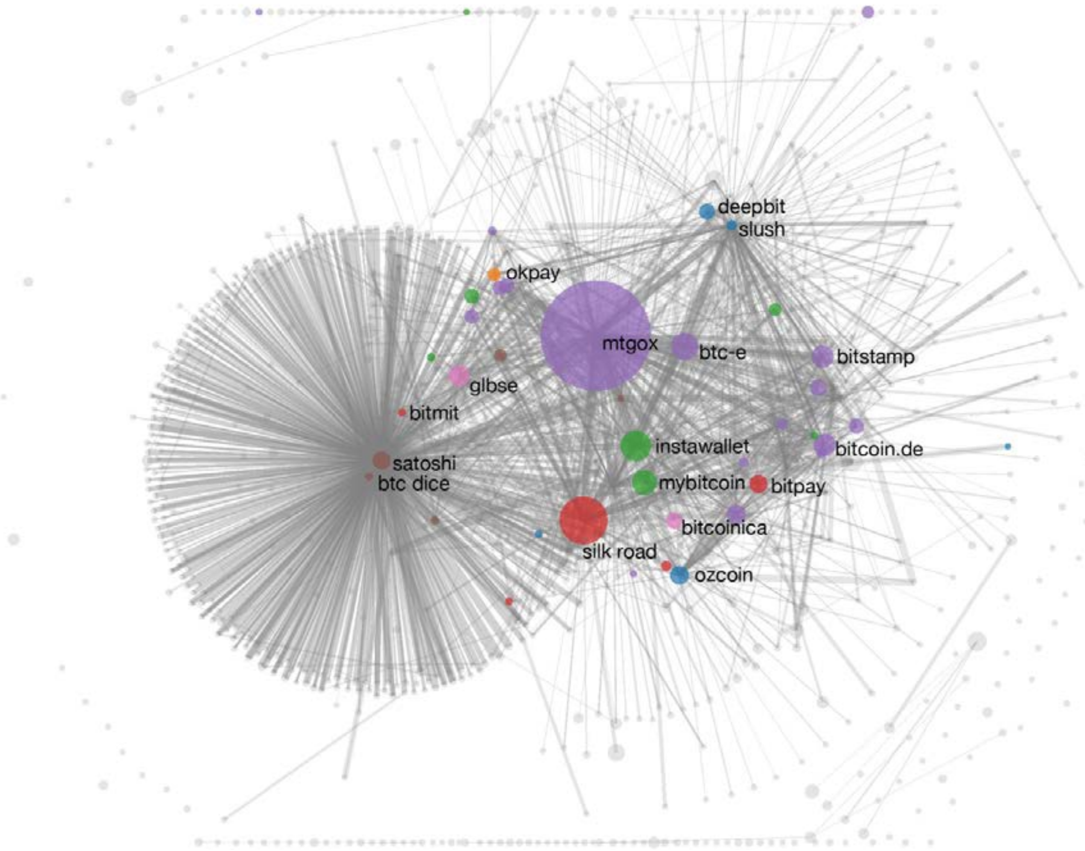


Scenario 1:
Shared spending

Scenario 2:
Change Address

Shared spending and change address can provide evidence of joint control

Linking Bitcoins in the Wild



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

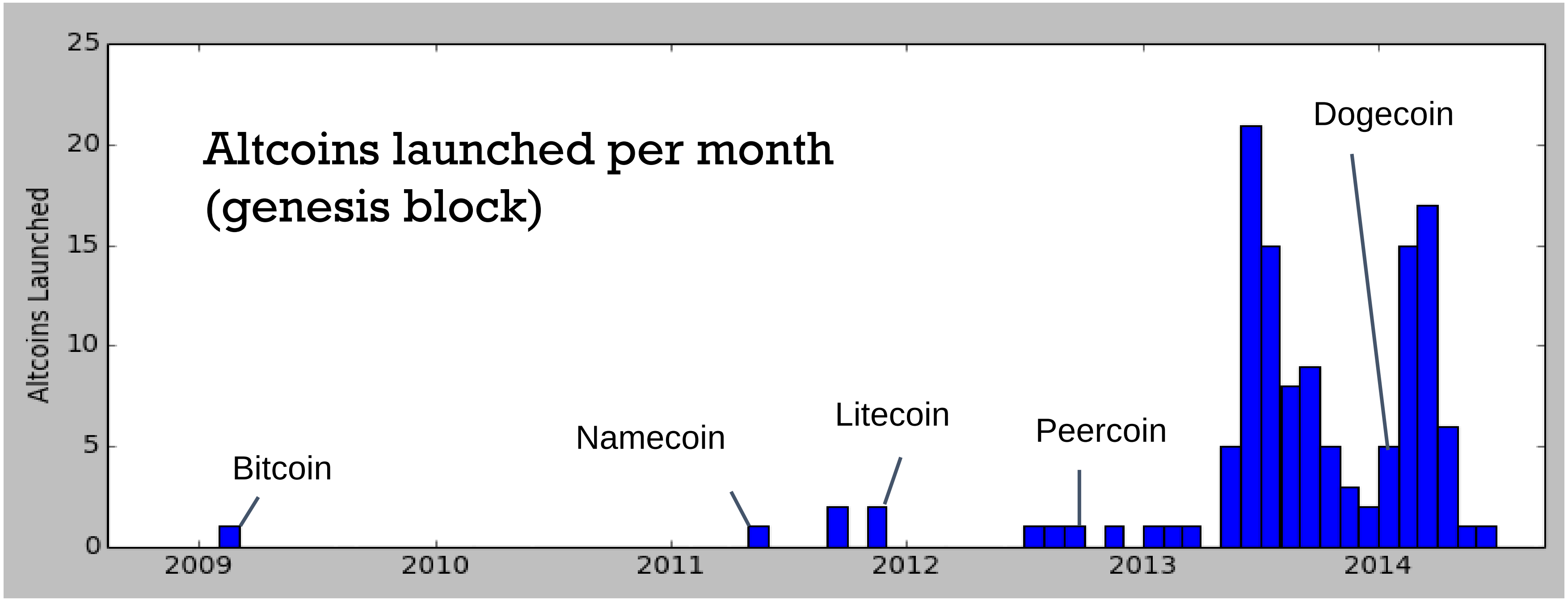
S. Meiklejohn et al.

Talk Outline

- Crypto Background
- Bitcoin Details
- What's Next

Bitcoin is Not Alone!

As of 2015, 50-500 altcoins launched!



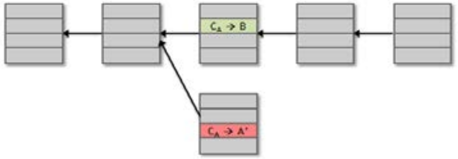
Data from mapofcoins.com

Reasons for Altcoins

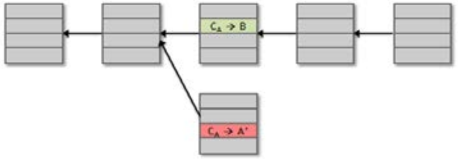
- Better (or different) security.
  - Mining puzzle.
- Contract/platform features.
- Different parameters and monetary policy.
  - Inflation.
  - Inter block time.
- Community or common interest support.

Bitcoin's Blockchain Platform

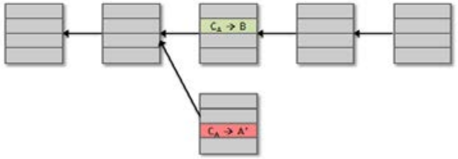
- Works only for Bitcoin!
- **<u>How to implement a distributed application with a slightly different logic/requirement?</u>**
  - Create a new blockchain to support the application!
- Result:



Bitcoin



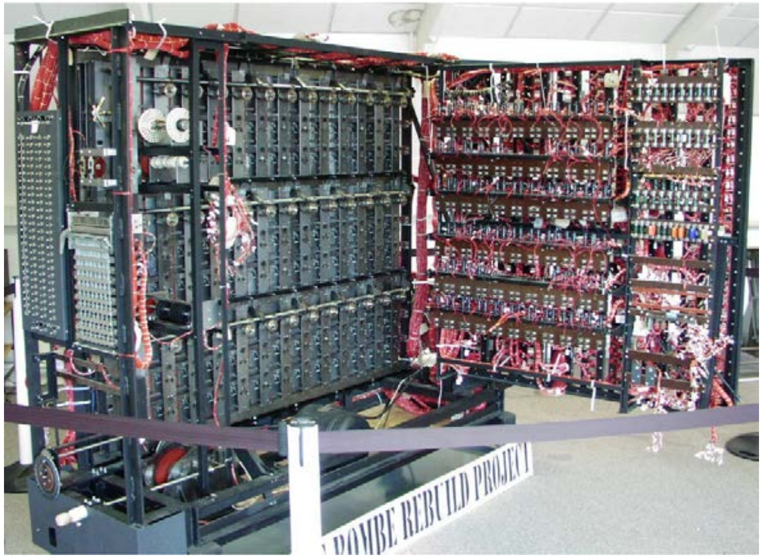
Litecoin



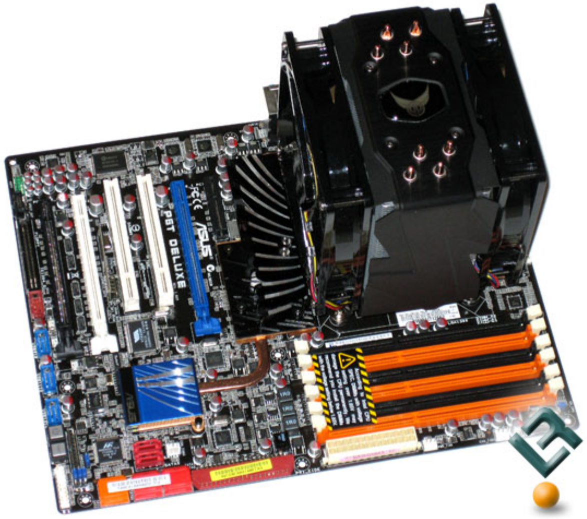
Dogecoin

Question: Can we build a single blockchain that supports multiple distributed applications?

Bitcoin's Blockchain Platform - Analogy



Versus



Smart Contract Model in Ethereum

- Notion of accounts:
  1. Externally Owned Accounts (governed by users).
  2. Contract Accounts (governed by contracts or code).
- Smart Contract: A program that lives on the Blockchain (forever).
  - Written in Solidity – a high-level programming language used by Ethereum.
- Anyone can create a contract and upload it.
  - Pay a small fee, done by means of a special "transaction".
- Users send "specially crafted" transactions to execute these contracts.
- Miners agree on order of transactions and actually execute contracts using a PoW-based consensus.
- Ethereum clients run a special virtual machine, called EVM, which executes the smart contracts.

Two types of Blockchain Applications

- Public Blockchains:
  - Blockchain participants are not authenticated.
  - Anyone can participate (also referred to as permission-less blockchains).
  - Example: Bitcoin, Ethereum.

- Private Blockchains:
  - Blockchain participants are authenticated.
  - Only authenticated nodes can participate (also referred to as permissioned blockchains).
  - Example: Hyperledger framework by IBM.

Moving Forward – Main Innovations

- Incentives: Why should users participate?
- Scalability: How to increase number of transactions per second?
- Space: How to reduce the size of the Blockchain?
- Applications in other domains/businesses: For authentication, integrity, record-keeping, etc.
  - IoT
  - Supply Chain
  - Financial Services
  - Spectrum Management
  - ……

Thanks for your attention!