CITP

CITP.PRINCETON.EDU

DataX

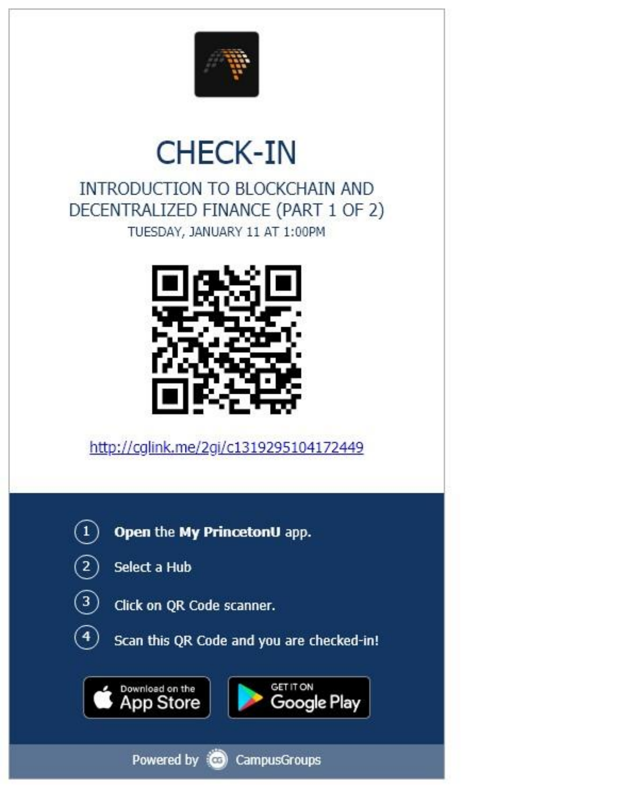
Introduction to Bitcoin

PRANAY ANCHURI

PREPARED FOR WINTERSESSION-2022

Logistics

CHECK-IN
@ HTTP://CGLINK.ME/2GI/C1319295104172449



CHECK-IN

INTRODUCTION TO BLOCKCHAIN AND DECENTRALIZED FINANCE (PART 1 OF 2)
TUESDAY, JANUARY 11 AT 1:00PM

http://cglink.me/2gi/c1319295104172449

1. **Open** the **My PrincetonU** app.
2. Select a Hub
3. Click on QR Code scanner.
4. Scan this QR Code and you are checked-in!

Powered by CampusGroups

Goals of this session

- Briefly look at historical and current monetary systems, and learn how they compare against Bitcoin
- Learn basic cryptographic primitives used in Bitcoin
- Understand how Bitcoin works
- Applications beyond value exchange on Bitcoin
- Setup for next session where we will look at Ethereum and Decentralized Finance products

About me

DataX Data Scientist at the Center for Information Technology Policy, SPIA

PhD in Computer Science, Rensselaer Polytechnic Institute

Worked as Blockchain Research Scientist at Axoni, NYC.

Research areas :

- Blockchain
- Network analysis
- Machine learning

Outline

- History of money
- Cash
- Cryptographic primitives
- Bitcoin
- Demo

Outline

$

History of money

Money

- Asset used to purchase goods and services
- Roles:
  - Value goods
  - Medium of exchange
  - Store of value
- Historically, people exchanged goods even in the absence of a specific medium
- To understand money, we need to look at monetary systems used by societies to value and exchange goods

Terminology

Monetary system

- Units of value and medium of exchanging value
- Key elements in a functioning market economy

Unit

- Quantity of economic value
- All items in the economy can be priced as multiples of unit

Medium of exchange

- Item whose value is proportional to the unit
- Easy to store
- Obtains value from its acceptance, purchase power

Four phases

Transition from a medium coupled with commodities to credit money

Phase 1

COMMODITY MONEY

Commodity money

- Units were usually well-known or prestigious commodities
  - Bushel of grains, precious metals
- Lack of wide availability meant commodities are reserved for high-value transactions
- Everyday transactions relied on
  - Bilateral credit
  - Non-standard commodities
- *Transition to a standard unit and state issued coins*

Phase 2

RISE OF COINAGE

Coinage

- State issued precious coins became medium of exchange
  - State ascertains weight and quality of coins
- Standardization meant that low-value transactions are possible
- Coins represent more than the metal it contains
- State vs public

State	Public
Project sovereignty	Less value outside the state
Can create money by using lesser metallic content	Less intrinsic value
Source of revenue	Acceptance of tax obligations

- *Transition to a more available medium*

Phase 3

CREDIT MONEY

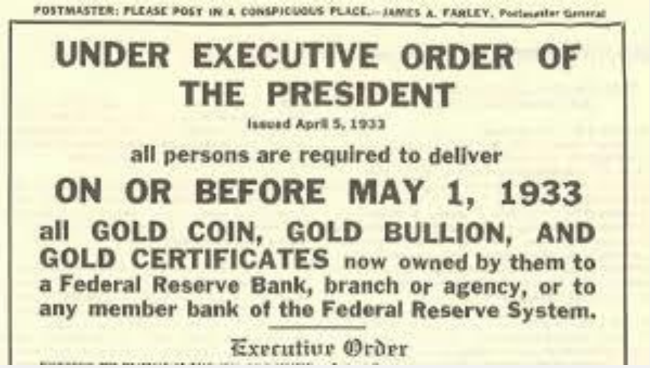
Credit money

- Coinage was successful except for the wide availability (People were still using bilateral credit)
- Ancient banks - People gave up ownership of coins and receive debt against bank, deposit money
- Introduction of modern banks (central and commercial)
  - Credit money – Banks were allowed to "create"/loan money even without an associated deposit of coinage
  - Promise to exchange for precious metals on demand; Banks were required to keep a fraction of total value, lending business
- Widespread usage when government accepted notes for taxes
- *Transition to credit money without convertibility*

Phase 4

NO MORE GOLD STANDARD

Modern system



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

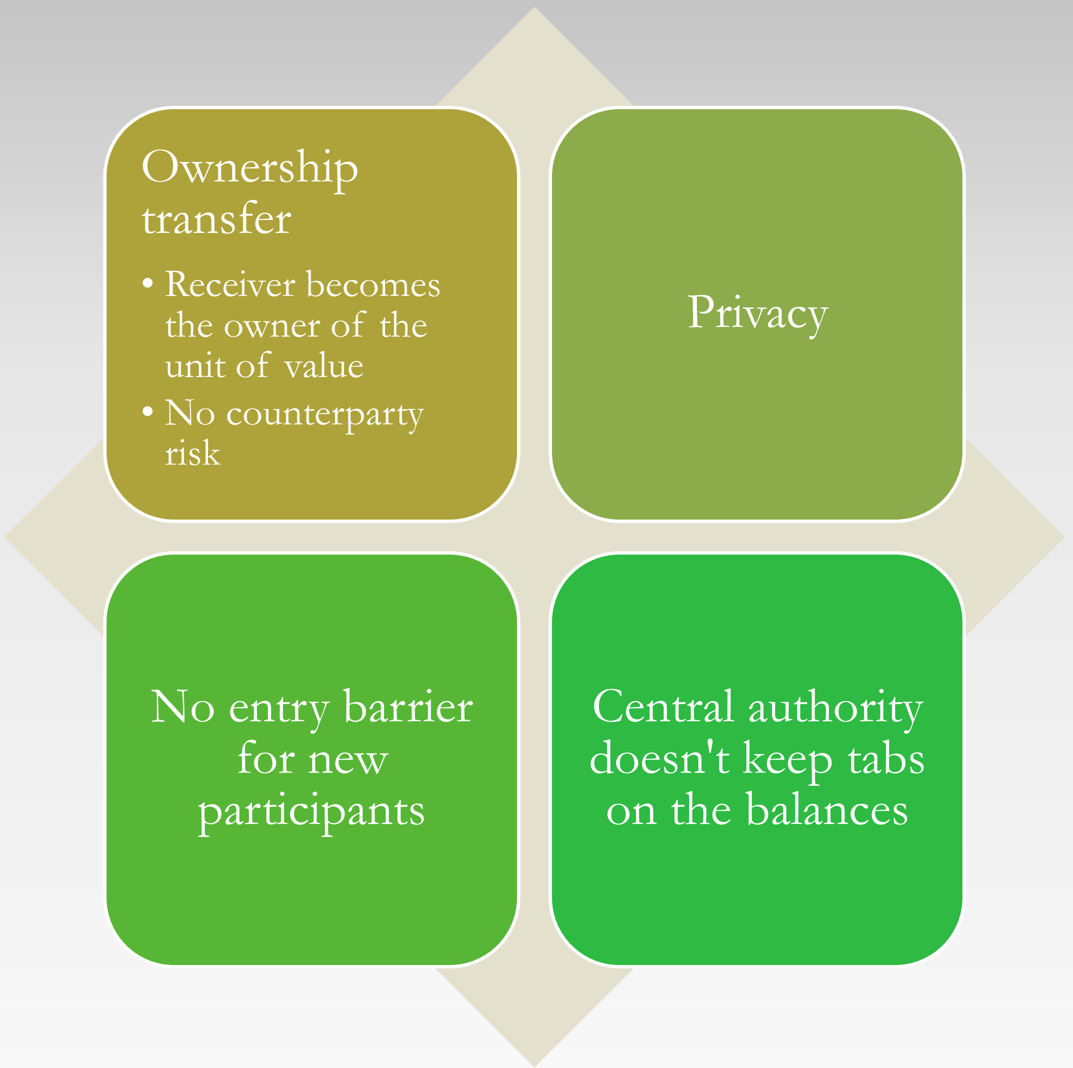
- Difficult to support convertibility to Gold
  - State cannot pump-in money during emergencies
- After wars and economic crisis gold conversion was abandoned
- State ensures paper money is accepted
- Availability problem is solved
  - New problem – excess availability

Outline

History of money

Cash

Cash as a medium of exchange



Ownership transfer

- Receiver becomes the owner of the unit of value
- No counterparty risk

Privacy

No entry barrier for new participants

Central authority doesn't keep tabs on the balances

Physical cash vs Digital cash

Physical cash

- Cash exchanges requires both parties to be at same location
- Limited denominations makes handling cash tedious
- Difficult to transfer large amounts

Digital cash

- +Digital version of cash and transfers
  - Venmo, PayPal, Zelle
- +Allows cross border transfers
  - Xoom
- -Requires a central authority (bank) to maintain account balances
- - Not everyone is banked yet!

Electronic cash with properties of physical cash

Why ?

- Ease of electronic cash
- Privacy of physical cash

DigiCash

- Earliest attempt at a digital version of cash with spender privacy
- Banks issue tokens which can be redeemed later. Deposits and redemption cannot be linked
- Failed for a variety of reasons
  - Ahead of its time – ecommerce was still in early stages
  - Banks were not onboard

Bitcoin is the first digital cash which can function without any central authority!

What is Bitcoin

- A monetary system without a central authority (state)
- Unit of value : Bitcoin/Satoshi 100 million Satoshi = 1 Bitcoin
- Medium of exchange is a data file that proves ownership of Bitcoins
- Pre-defined supply
- No intrinsic value (like current CB issued currencies)

Monetary system without a central authority

YAPNESE STONE MONEY

Decentralized economy of Yap island

PEOPLE KNOW EACH OTHER

MILLSTONE LIKE STONES ARE USED IN VALUE EXCHANGE

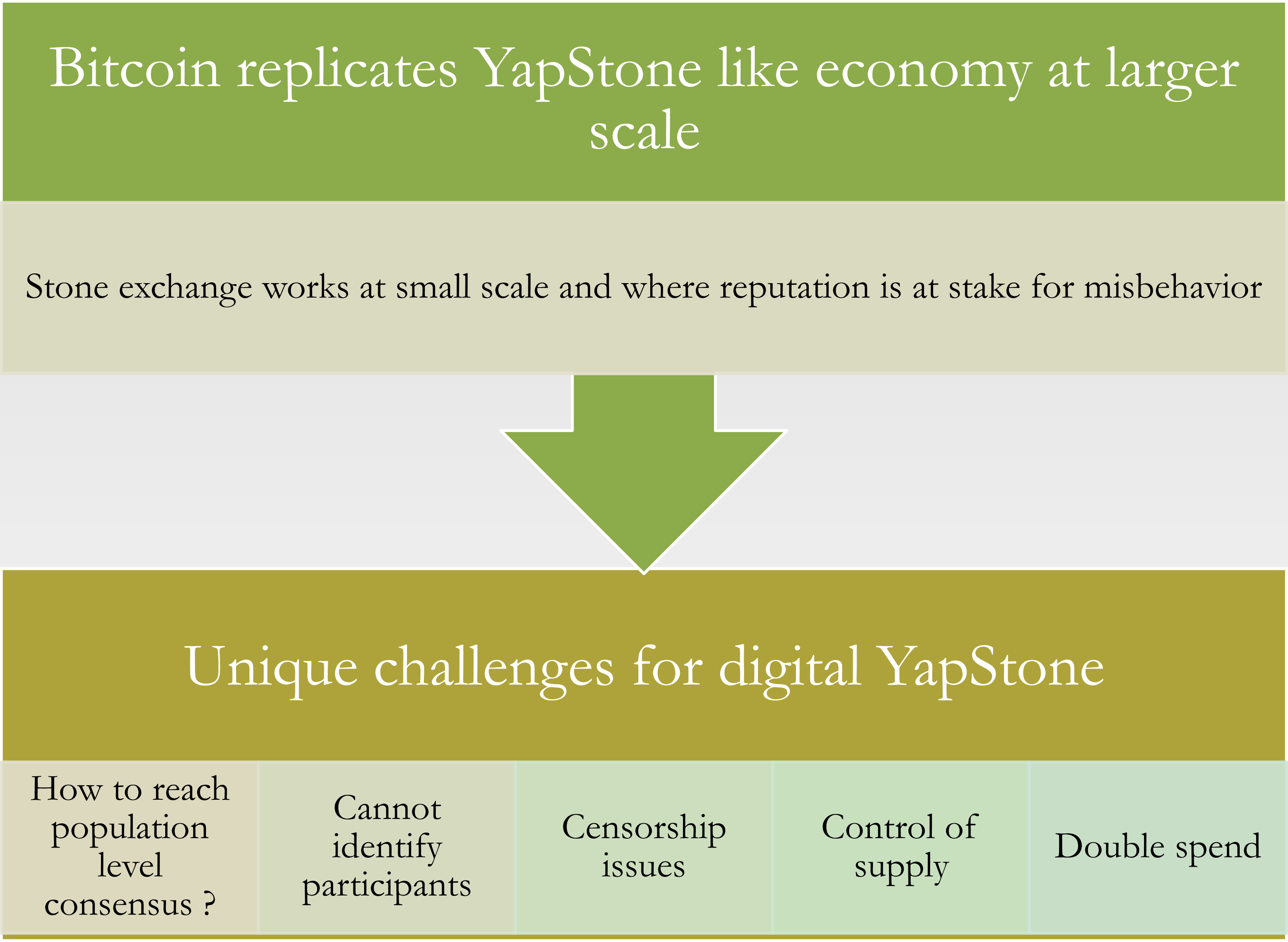
ANYONE CAN BRING STONES TO THE ISLAND

EVERYONE KNOWS WHO OWNS WHAT

PAYMENTS ARE GOSSIPED THROUGHOUT

CONFLICT RESOLUTION

YapStone vs Bitcoin



Bitcoin replicates YapStone like economy at larger scale

Stone exchange works at small scale and where reputation is at stake for misbehavior

Unique challenges for digital YapStone

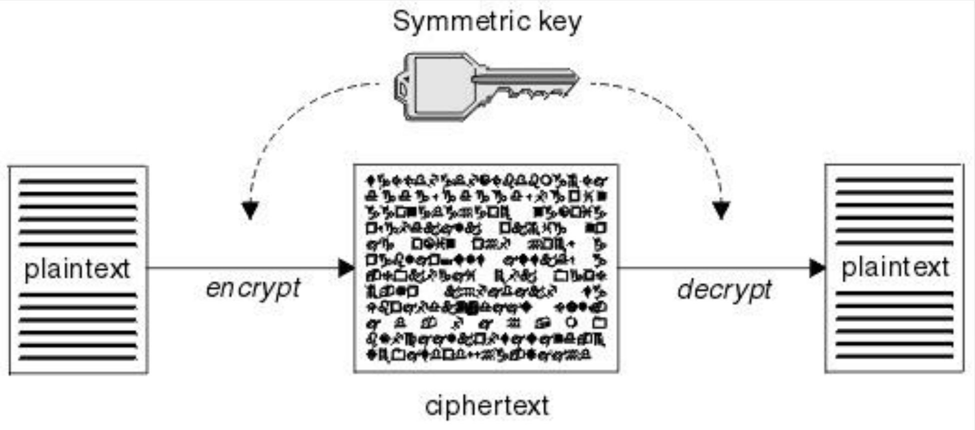
How to reach population level consensus ?	Cannot identify participants	Censorship issues	Control of supply	Double spend

Outline

- History of money
- Cash
- Cryptographic primitives

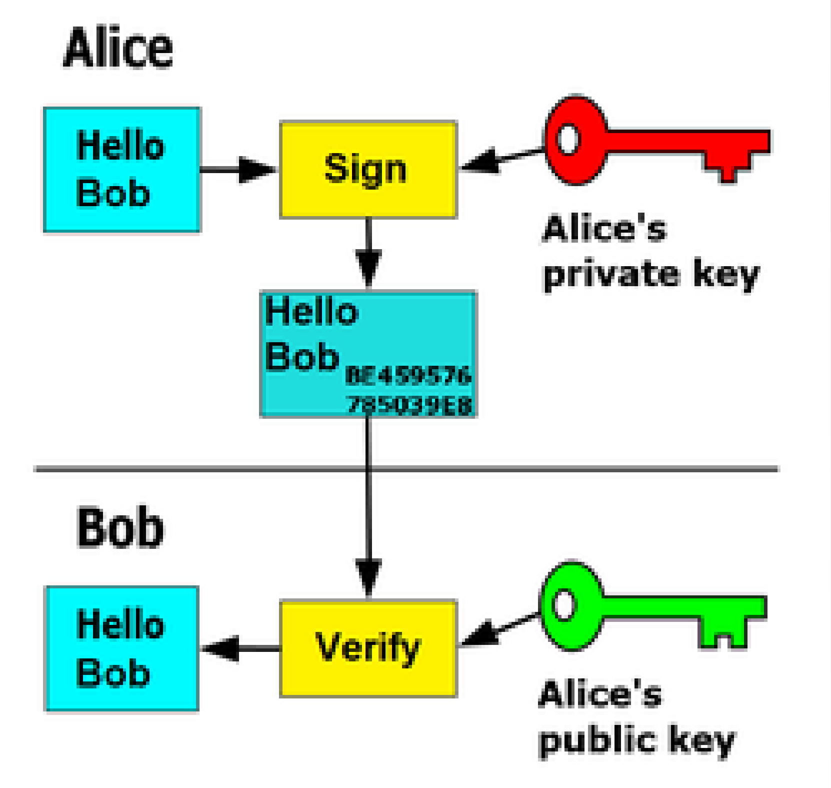
Symmetric key encryption

- Same key to encrypt and decrypt
- Used during WW2



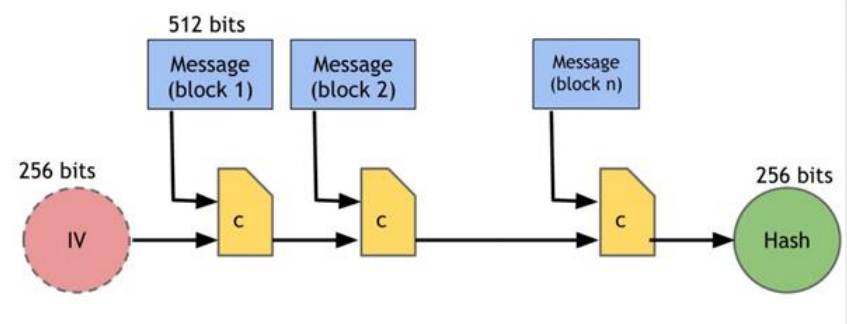
Asymmetric key based signature

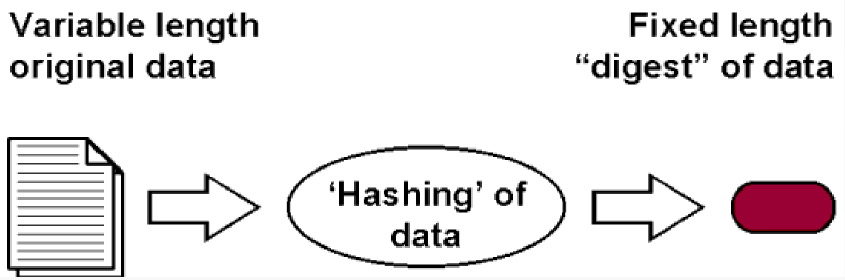
- Key has two parts : Public key and private key
- Public key is used an identity
- Private key has two uses
  - Decrypt messages sent to corresponding public key identity
  - Sign messages to prove ownership of a private key



Cryptographic hash

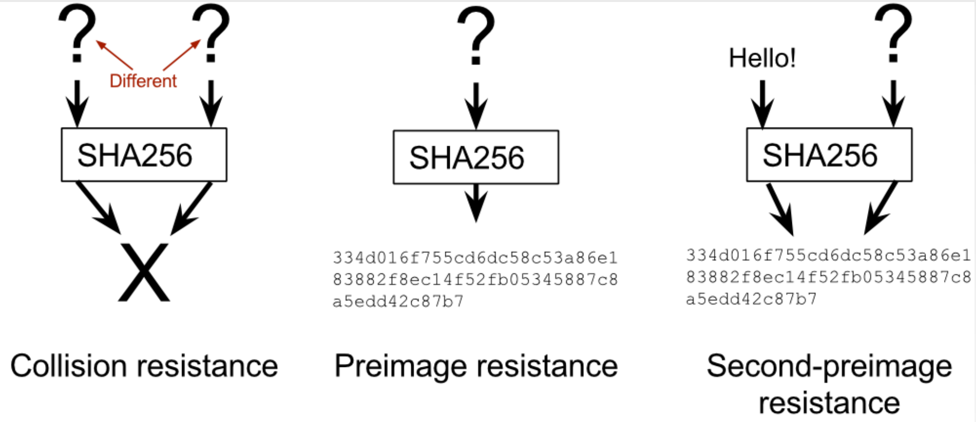
- Hash is a mathematical function (h) that maps any data to fixed length summary
- Used to uniquely identify transactions
- Not all mapping functions fit requirements





Properties of hash function

- Collision resistance
  - Difficult to find d and d', h(d) = h(d')
- Pre-image resistance
  - Given the hash digest 'm', it's difficult to find data 'd' such that h(d) == m
- Second pre-image resistance
  - Given h(d) = m, it's difficult to d' such that h(d') = m


?
?
Different
SHA256
X
Collision resistance
?
SHA256
334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7
Preimage resistance
Hello!
?
SHA256
334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7
Second-preimage resistance

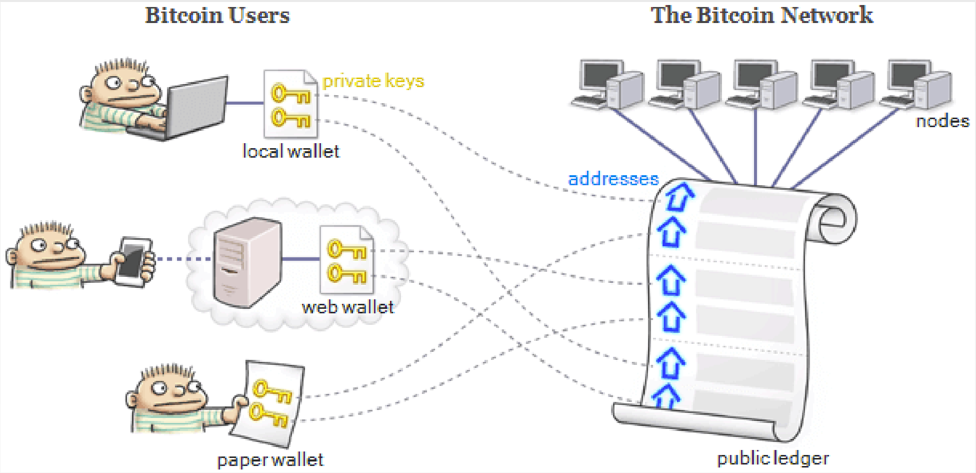
BREAK

Outline

- History of money
- Cash
- Cryptographic primitives
- Bitcoin

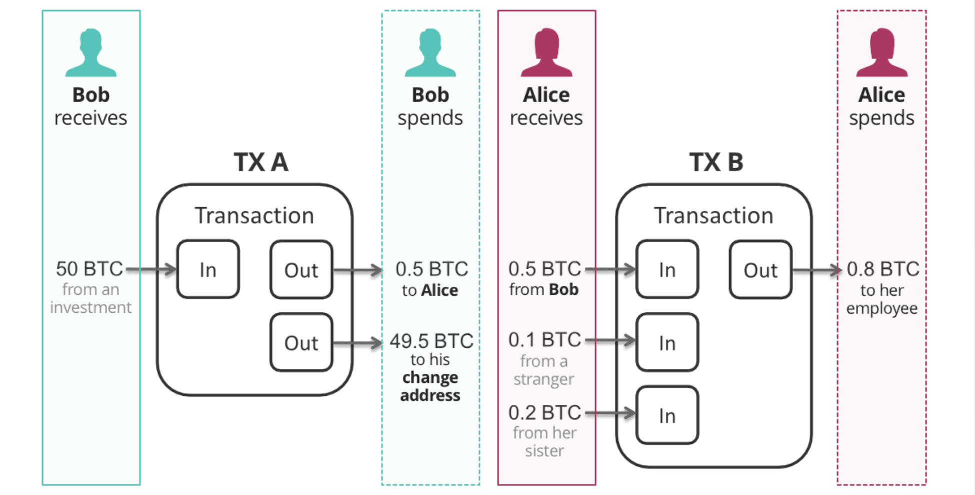
Bitcoin from the ground up

- Transactions
- Public ledger
- Dealing with fraud
- Introducing value into system



Transactions : Value exchange

- Each bitcoin is associated with a public key
  - Anyone who can sign a message that tallies with the associated public key is its owner
  - Cryptographic keys are not tied to real-world identities
- Owner can initiate a transfer by signing a message that transfers ownership to a different public key
- Multiple inputs and outputs per transaction
  - Value must be conserved



Bitcoin network : Gossip payments

Transactions gossiped by Bitcoin nodes

Transaction can be duplicated without the risk of modification

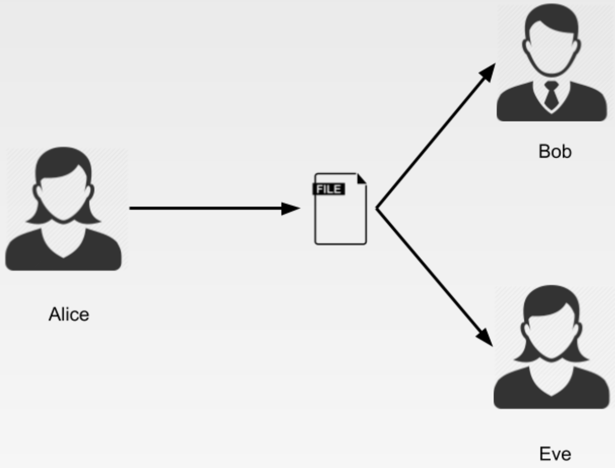
Signature invalid if any part of the transaction is modified

Avoid censorship by sending transaction to nodes distributed throughout the world via internet

Satellites to avoid dependence on internet

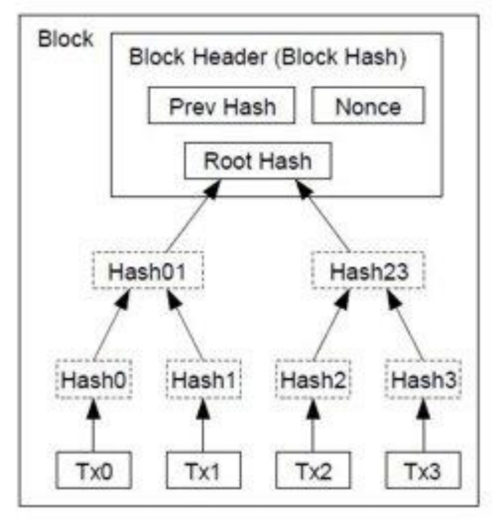
Ordering transactions : Fraud prevention

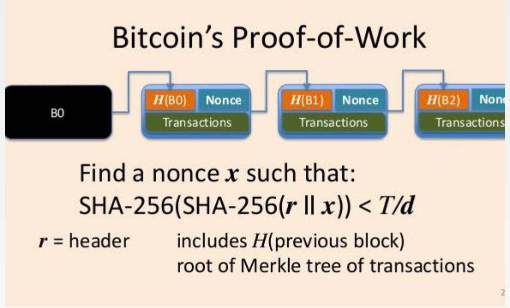
- Everyone keeps a record of all the unspent Bitcoins in circulation
- Double spend problem
  - ***Alice*** pays the same Bitcoin to ***Bob*** and ***Eve***, simultaneously
  - No central authority to decide correctness
- Anyone can participate in deciding the order
- A game theoretic approach to incentivize correct behavior and penalize misbehavior



Proof-of-work

- Transactions are grouped into blocks
- Miners solve hash-based puzzles for the ability to propose new blocks
  - Probability of solving the puzzle is proportional to the amount of computing power
- Similar approach was used in combating spam
  - Solve puzzle before sending an email




B0
H(B0)
Nonce
Transactions
H(B1)
Nonce
Transactions
H(B2)
Non
Transactions

Bitcoin's Proof-of-Work

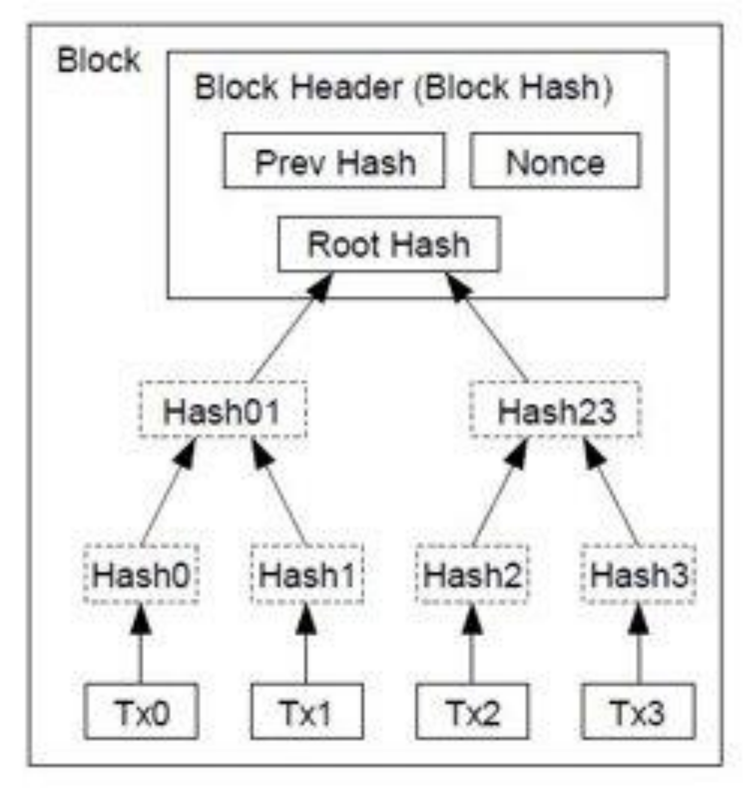
Find a nonce x such that:
SHA-256(SHA-256($r \| x$)) < T/d

r = header includes H(previous block)
root of Merkle tree of transactions

SHA256 and Proof-of-work demo

Mining incentives : Introducing value

- Miners are rewarded for including transactions
  - Pay what you wish model
- Miners also create a special *Coinbase* transaction (that assigns new bitcoins to self)
- Miners transmit newly minted blocks to the network



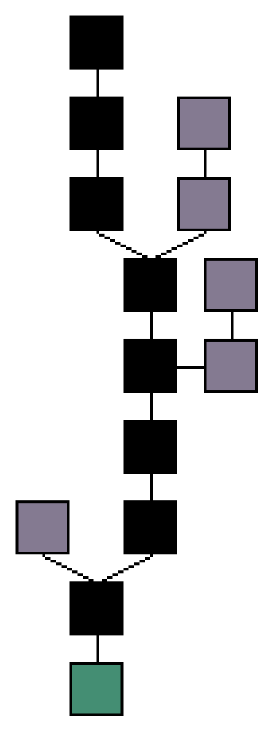
Consensus : Progress

- Forks can happen even with perfect incentives

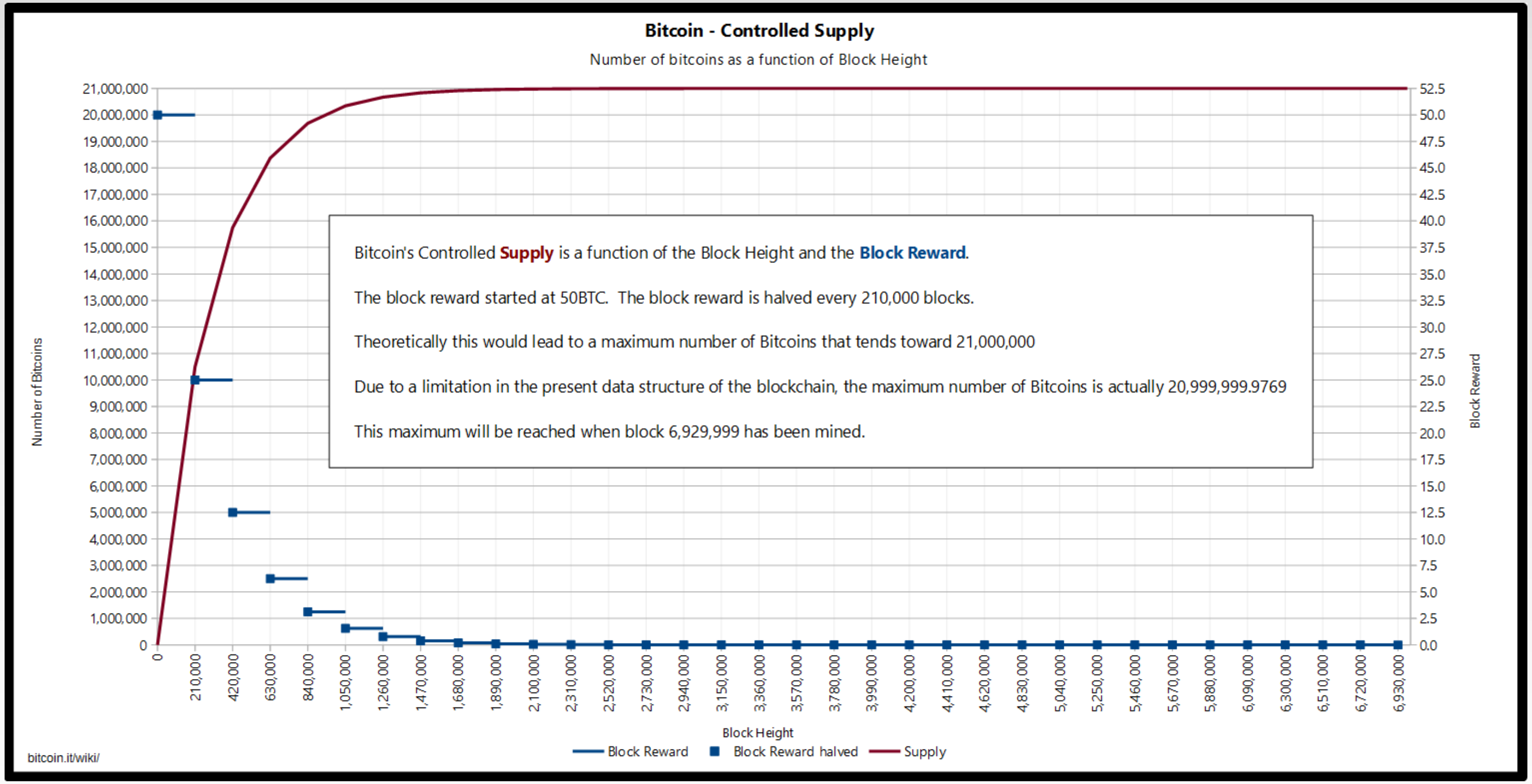
- Future puzzle solvers are free to choose to link their block from any point of the chain
  - Blockchain is more of a tree

- The consensus is that the largest chain is the "correct" version of history

- Rational miners want to participate in the correct version
  - Resources (used in solving hash puzzle) are wasted if subsequent blocks don't build on their blocks



Controlled supply



Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

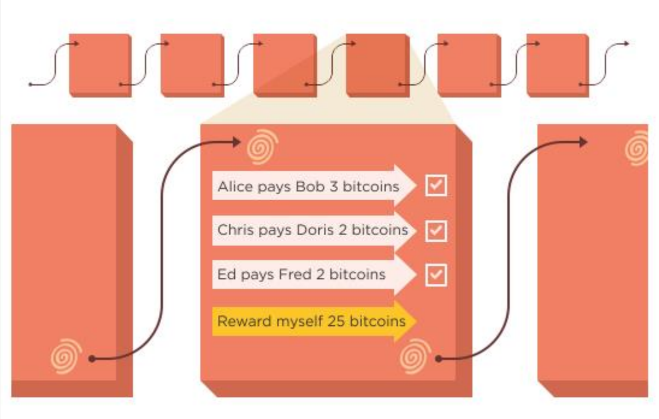
Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Putting it all together

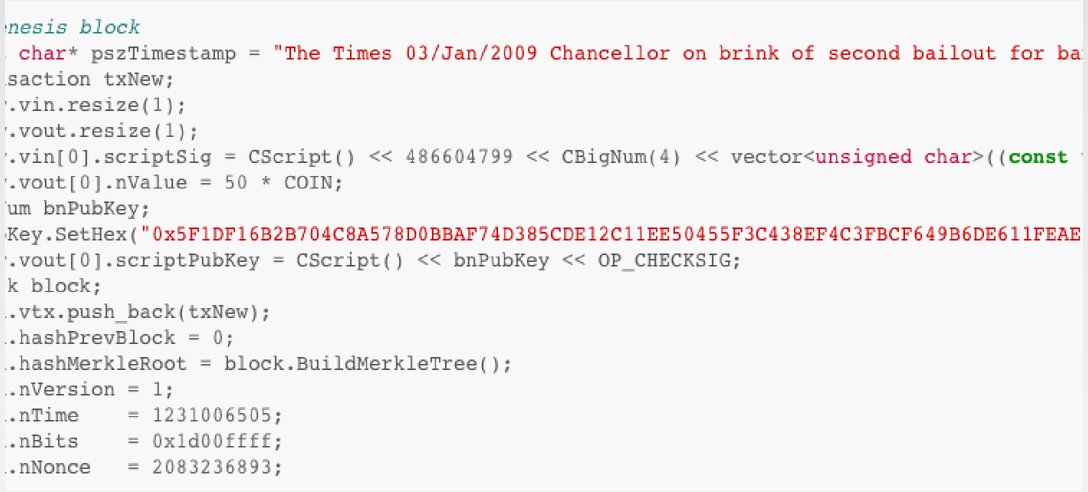
- Bitcoin blockchain is a decentralized value exchange system
- Users create public key-based identities
  - Suggested to create a new identity for each transaction
- Transfer ownership of bitcoins by signing a transaction with private key
- Miners accumulate transactions, solve hash-based puzzles to order the transactions
  - New bitcoins are introduced via mining rewards
- Everyone updates their copy of the blockchain


Alice pays Bob 3 bitcoins ☑
Chris pays Doris 2 bitcoins ☑
Ed pays Fred 2 bitcoins ☑
Reward myself 25 bitcoins

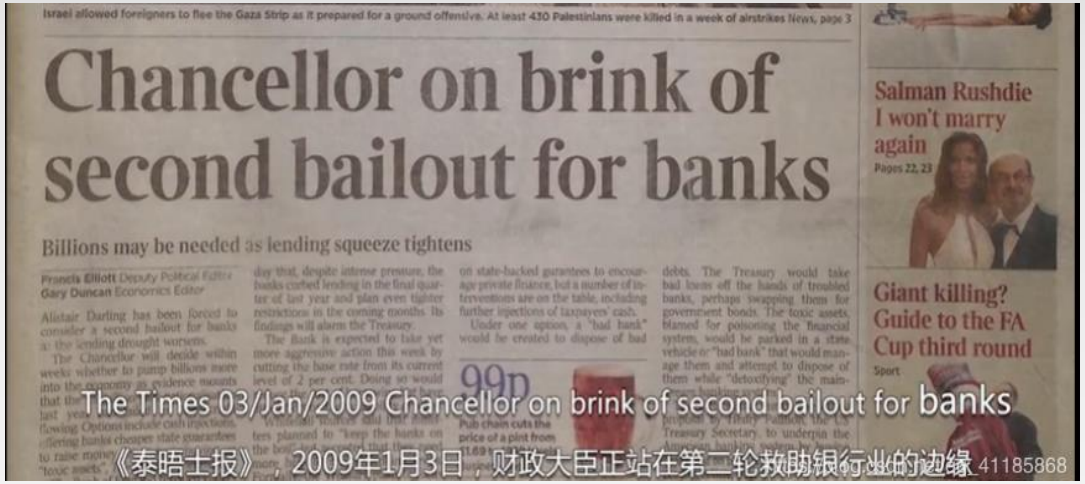
Properties of Bitcoin

- Censorship resistance
- Permissionless
- Fungibility
- Anonymity
- Fixed supply
- Minimal centralization risk

Origin of Bitcoin



```
nesis block
 char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout for ba
saction txNew;
.vin.resize(1);
.vout.resize(1);
.vin[0].scriptSig = CScript() << 486604799 << CBigNum(4) << vector<unsigned char>((const
.vout[0].nValue = 50 * COIN;
um bnPubKey;
Key.SetHex("0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE611FEAE
.vout[0].scriptPubKey = CScript() << bnPubKey << OP_CHECKSIG;
k block;
.vtx.push_back(txNew);
.hashPrevBlock = 0;
.hashMerkleRoot = block.BuildMerkleTree();
.nVersion = 1;
.nTime    = 1231006505;
.nBits    = 0x1d00ffff;
.nNonce   = 2083236893;
```



Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the

day that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would

on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the main-

99p

Pub chain cuts the price of a pint from

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

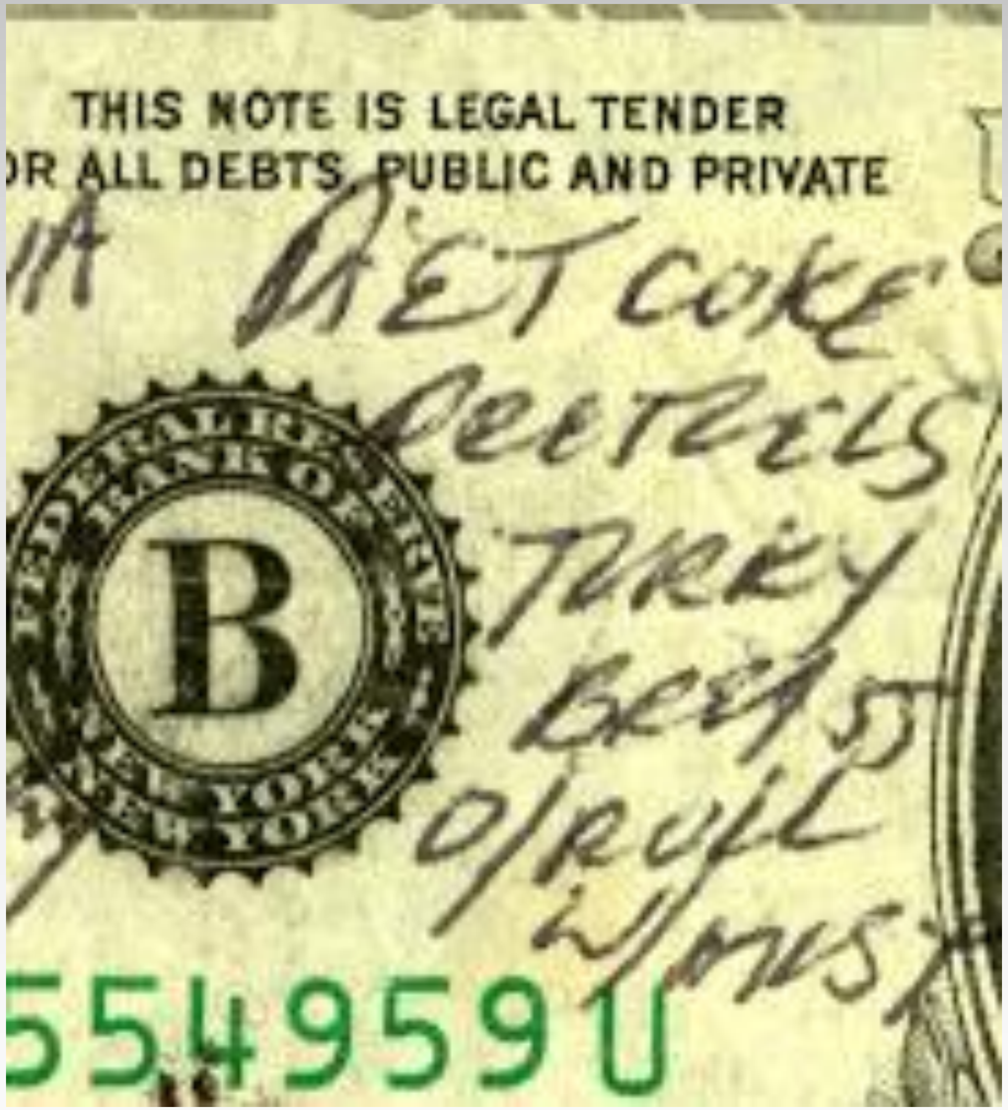
《泰晤士报》，2009年1月3日，财政大臣正站在第二轮救助银行业的边缘

Inspecting a bitcoin block

BLOCK 717935

Applications

BEYOND VALUE TRANSFER


THIS NOTE IS LEGAL TENDER
OR ALL DEBTS, PUBLIC AND PRIVATE
DIET COKE
TURKEY
Beef
FEDERAL RESERVE BANK OF NEW YORK
NEW YORK
B
554959U

Colored coins

Colored coins are bitcoins annotated with a special meaning

Linking physical assets like tickets, airline miles etc.

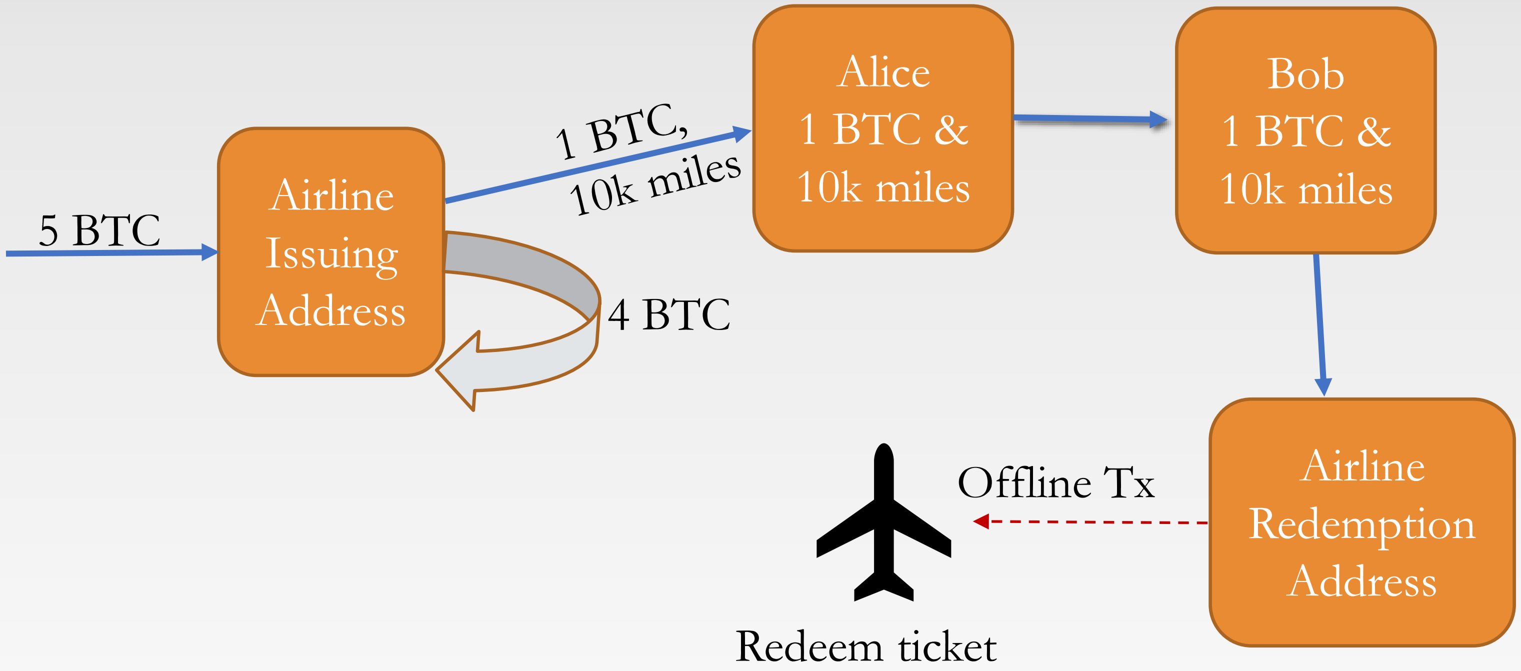
Uses Bitcoin infrastructure to easily transfer, trace etc.

Colored bitcoins can hold more value

Issuer risk

Colored coins have value only if the issuer accepts them

Colored coins example



Outline

- $ History of money
- Cash
- Cryptographic primitives
- ₿ Bitcoin
- ▶ Demo

Challenges

- Fierce competition among miners to solve proof-of-work puzzles
  - Around 6.25 BTC/~250k USD per block at stake
  - Requires huge amounts of energy per block
- Bitcoin network processes around 10 transactions per second
  - Visa throughput is around 10k transactions
- Transactions are not completely anonymous

Recap

- History of money
- Origins of digital cash
- Bitcoin protocol
- Applications
- Next part : Ethereum and Decentralized Finance

Announcements

- https://forms.gle/jCzCL6bWN8cr8S4G6 - optional survey