Crypto-currencies & Bitcoin
Peer-to-Peer Systems and Security (IN 2194)

Sree Harsha Totakura
Technische Universität München

April 29, 2014
Definitions

Coin
A metallic object, often in circular shape, representing a tangible unit of wealth.

Bank Note
A note is a promise certificate made by a bank to the bearer that it owes an amount of wealth equal to the face value printed on the note.

Currency
Coins and bank notes which are accepted as money by a society (or nation) are collectively termed as currency for that society (or nation).

Money
Liquidated wealth which can be readily exchanged for goods or services.
Definitions

**Asset**
Anything which can be liquidated to money or traded upon is an asset. Money is also an asset.

**Wealth**
Wealth is the value of all assets.

All of these terms are casually misused
Money, Money and, Money

long long ago  Barter trade, debt-based ledger
long ago  Commodity money: bags of wheat
metal age  Representational money: coins, banknotes
1958  Digital money
now  Crypto money

What is the difference between digital money and crypto money?

crypto money ⊂ digital money
Money Creation

“Let me issue and control a nation’s money and I care not who writes the laws.”

— Mayer Amschel Rothschild (1744-1812)
Money Creation

Central Bank
An authority to manage a state’s currency, money supply and interest rates.

Commercial Bank
The bank with which people or businesses interact with for saving their money, getting loans, etc. Commercial banks are in many cases overseen by their state’s central bank.

Mint
Money factory. This is where coins are minted and currency notes are printed.

- Mint can be under the control of central bank (Reserve Bank of India) or government (U.S. Department of Treasury)
- Money created at a mint always go to the central bank which oversees its circulation
Money Creation — Gold Standard (pre 1974)

- Mint creates coin and paper currency based on national gold reserves
- Central banks place the created money into circulation
- Commercial banks lend the money to its customers
This is a promissory note. It is a promise to pay at some point in the future. When you use one of these to purchase goods, all you are doing is exchanging a debt with more debt. The banks that issue these promissory notes charge interest for doing so, which you pay for with your income tax. Essentially, your labor is used as collateral on the debt the government owes the banks for lending them their notes. And by pumping this fake money into the economy it creates inflation which devalues your spending power.

Pissed off yet?
Money Creation — Now

- Mint creates coin and paper currency out of nothing
- Central banks place the created money into circulation
- Commercial banks lend the money to its customers
- Additionally, commercial banks also create large proportions of money through Fractional Reserve Banking
Fractional Reserve Banking

Balance ledger

A list maintained by a bank consisting of all transactions made upon its customers’ accounts.

- Alice deposits 100 in her bank
- The bank notes this in its Balance ledger
- The bank keeps 10 in its safe and offers 90 as loan to Bob
- The total money in the system is now $100 + 90$
- Bob deposits his 90 in his bank.
- Bob’s bank keeps 9 in its safe and offers 81 as loan
- The total money in the system is now $100 + 90 + 81$
- And the cycle continues further ...
- Eventually, Bob repays his loan with interest (profit for Alice’s bank)

The banks created money out of nothing based on the assumption that not all of its deposits will be withdrawn at the same time.
Are Banks Evil?

“Give a man a gun and he can rob a bank.
Give a man a bank and he can rob the world.”
— Internet Meme

Not necessarily, it depends on:

▶ Who owns the bank? Government, businesses, private individuals
▶ Who controls the bank? Government/private individuals, centralised/decentralised
▶ Who gets the profit? Profit pumped back into the economy?
Issues with Representational and Digital Money

- Counterfeiting
- Privacy
  - Unlinkability towards merchant: can merchant’s data mine on customers transactions to identify a customer’s purchasing trend?
  - Unlinkability towards bank: can bank get to know what a customer has bought?
  - Unlinkability towards state: can a person transfer/receive money without the state knowing it: tax evasion
- Enforcing contracts
  - pay and get no service
  - get service and evade from paying
  - Escrow payments
Crypto-money/Crypto-currency

A monetary system where creation of money and its distribution involves usage of cryptographic primitives.

Advantages:

▶ Hard to counterfeit as (well implemented) crypto is hard to break
▶ Designs incorporating cryptography allows us to provide privacy
▶ Cryptographic signatures make it easy to verify transactions/contracts

However, there are other problems...
Who should be allowed to add new crypto-money into circulation?
How should the money supply be controlled?

- An “independent” central bank?
- Through a *technologically*-controlled process that NOBODY can influence
POW should be hard to do, but easier to verify

Example

Find a value that when hashed through SHA256 produces an output with 52 leading bits unset

- SHA256 has 256-bit output → $2^{256}$ different outputs
- Number of outputs with leading 5 unset bits = $2^{204}$
- Probability of find an output with 5 leading unset bits for a given input = $1/2^{52}$
- A single call to SHA256 is enough to verify any solution
Double-spending Problem

1. Alice has 10 units of money
2. Alice paid Bob 10 units of money and now has no more money.

What prevents Alice from paying Carol the same 10 units of money?

▶ Representational currency: Alice gives away the currency notes to Bob
▶ Digital currency: Alice’s bank transfers Alice’s digital money to Bob’s bank

Wait, this is easier said than done.
What is to happen when due to some protocol exception Alice’s bank transfers Alice’s money to Bob’s bank but Bob’s bank does not receive it?

We need transactions with ACID properties.
CAP Theorem [1]

No distributed system can \textit{consistent}, \textit{available} and \textit{partition tolerant} at the same time.

\textbf{Consistency} A \textit{read} sees the changes made by all previous \textit{writes}.

\textbf{Available} \textit{Reads} and \textit{writes} always succeed.

\textbf{Partition tolerance} The system operates even when network connectivity between components is broken.
With digital currency, the transfer can only happen when both banks acknowledge the transfer. From the CAP Theorem, banks can therefore choose to have:

- **CA** Inter-bank transactions fail when either one of the bank’s system is down or the network connection is broken
- **CP** Inter-bank transactions are delayed arbitrarily
- **AP** Inter-bank transactions always succeed, but not consistent. Banks never use this.

What about Crypto-currency?
Double-spending Problem — Crypto-currency

- Alice signs the payment for Bob
- Alice OR Bob publish this payment publicly (or to a trusted third party)
- Carol (or the third party) can infer that Alice paid Bob 10 units of money and now only has 10 units less

Figure: A transaction

What Carol (or the third party) does is to calculate the amount in Alice’s account from the balance ledger.
Note that:

- Signing a transaction alone cannot solve double-spending.
- Signing a transaction and including it in the balance ledger does.
- But, including a transaction in the balance ledger requires ACID properties.
Money creation by crypto-mining. Number of monetary units created is proportional to POW.

Transfer of money is by signing and broadcasting the signature to all peers.

Everyone has to maintain a consistent balance ledger.

Does not guarantee ACID properties.

b-money 2: a subset of peers maintain the balance ledger and publish it periodically via Usenets. (broadcast transactions)

Still does not guarantee ACID properties.
Blocks & Block chain

- Transactions from a period are collected into *blocks*
- Blocks are like pages in the balance ledger
- Blocks are linked to form a chain (the ledger book)

![Figure: A block](image-url)
Ensuring ACID properties for Crypto-currency

With a centralised server

1. Peers send transactions to the timestamp server
2. The timestamp server periodically generates a new block
3. With regard to CAP, the system has CP semantics (system is not available because writes only succeed after sometime)

But, we don’t want centralisation.
Ownership & Maintenance of Block Chain

In a decentralised crypto-currency system

- Who can generate blocks?
- When are new blocks added to the block chain?
- How is the blockchain distributed?
- Are blocks kept until eternity?
**Bitcoin Block Chain**

![Diagram of Bitcoin block chain]

**Figure:** Block chain in Bitcoin

- Similar to block chain implemented with a central timestamp server
- Blocks can be generated by anyone. However, they need proof-of-work (block has to be mined)
- Block generation is not periodic but probabilistic
- What’s the incentive for generating blocks?
- **Block generation creates new coins!** The first transaction in a block is for crediting generated coins to the block’s miner
**Transactions in Bitcoin Network**

**Figure:** Transactions involving fractions of units

Transactions can have multiple inputs and multiple outputs
New transactions are broadcast (best-effort) to all peers
Each node collects new transactions into a block
Each node (or a group of nodes collectively) works on finding a POW for the block
When POW is found, the block is broadcast to all nodes
Nodes accept block only if all transactions in the block are valid
Nodes express their acceptance of the block by working on creating a new block with the hash of the accepted block
How does Bitcoin block chain address CAP?

- Bitcoin tries to achieve eventual consistency
- From CAP, this gives bitcoin CP semantics
- A block’s inclusion in the block chain does not mean that the block has ACID properties
  - An another peer can generate a different block at the same time → block chain branches
- Peers always work on the branch which is longest
- Longest branch is determined not by the length but by the total difficulty of the branch
The 51% Threat

“If an adversary has at-least 51% of network hashing power, they have full control of the network and modify the block chain at will”

This in incorrect. They can neither have full control of the network nor modify the block chain at will. They can however

▶ prevent new transactions from entering into block chain
▶ double spend the bitcoins they own
▶ make mining very difficult for other users

Bitcoin’s incentive discourages this type of attack:
▶ More hashing power $\rightarrow$ more bitcoins mined
▶ Why not play by rules and get equal/more benefit than attacking the system?
Target difficulty

Target difficulty is a number that determines the proof-of-work hardness for block generation. The POW should be less than this number for a block to be accepted.

- Target difficulty is inversely proportional to the number of blocks generated.
- In Bitcoin, target difficulty is calculated every 2016 blocks.
- Bitcoin adjusts the target difficulty such that blocks are generated every 10 minutes $\rightarrow$ target difficulty is calculated $\sim$ 2 weeks.
Target Difficulty

Figure: Bitcoin target difficulty

Source: http://bitcoin.sipa.be
Other Issues

- Transactions in Bitcoin are to be flooded to all peers
  - Bandwidth usage proportional to transaction volume
  - Small transactions can DoS the system
- Additionally, peers may reject a transaction
- **Transaction fees** gives an incentive for including the transaction and also to counter DoS
- All transactions have a minimum latency of ~10 minutes
Mining Profitability

Cost factors:

- Electricity
- Hardware costs
- Exchange rate
- Target difficulty
- Law of minimal profits from mining: is it profitable to mine bitcoins or just to buy them?
Operational costs: is BTC better than SEPA?

- Bitcoin block mining is expensive (energy = money)
- Compare with per transaction costs on IBM mainframes used by SEPA
Bitcoin’s built-in Deflation

- The number of generated bitcoins per block halves every 4 years
- This limits the total number of bitcoins that could be available to 21 million
- Bitcoins can get lost due to signing errors/software bugs
Privacy

All Bitcoin transactions are available globally

- Easy to track money flow
- Easy to track a seller/buyer once their pubkeys are identified
- Use multiple identities
  - Easy to data mine
- Use *laundries* – third party servers to mix bitcoins among users
  Laundry server has to be trusted
  - as not compromised
  - to return the bitcoins after mixing
Zerocoin

- Is a distributed laundry
- Cannot be mined
- Zerocoin-mint: Zerocoins are minted from Bitcoins of same (fixed) denomination (1 BTC = 1 Zerocoin)
- Zerocoin-spend: Upon payment Zerocoins can be converted back to Bitcoins
- A zerocoin-spend transactions gives out the same amount of Bitcoins, but not the same Bitcoins which were used for the corresponding zerocoin-mint transaction.
- Fractional denomination transactions not possible.
Taxability

Is taxation good? Yes, it is needed for:

▶ Building public infrastructure
▶ Education
▶ Healthcare
▶ Environmental protection
▶ Social benefits

Alternatives:
▶ Make the payer anonymous but not the recipient [3]
Alternative POW Algorithms

- Bitcoin uses SHA256 hash for POW
- Requires hashing power solely
- Many ASIC (Application-Specific Integrated Circuit) hardware implementations for efficiently finding SHA256 collisions available
  → Normal CPU/GPU mining rendered useless

Alternative POW Algorithms:

- Scrypt: requires memory in addition to CPU
- Memorycoin: requires a lot of memory → favourable for mining on desktop computers
Litecoin (LTC)

- Uses Scrypt
- No known ASIC hardware implementation as of now
- Limited coins
- Faster block generation; a block every 2.5 minutes
Dogecoin (DOGE)

- Similar to Litecoin (uses Scrypt)
- Steady inflation; unlimited coins
- Block generation every 1 minute
  → faster transaction confirmations, but more chances for block chain splits
Peercoin (PPC)

- Proof-of-work + Proof-of-stake
- Proof-of-stake means that coins are generated proportional to the coins held by the miner
- When target difficulty increases and mining becomes non-profitable, new coins are generated through proof-of-stake
- Steady inflation of 1% per year
- Unlimited coins
- Also has deflation; a transaction fees of 0.01 PPC is lost for every transaction
Questions
References

