The Latest Research on Bitcoin and Blockchain

Alfred Lehar
How does a blockchain work?
- Bitcoin
- Ethereum

How to buy crypto

Stablecoins

Impact on society

NOT on the agenda
- Should I buy Bitcoin?
- Will prices go up or down?
Blockchain, Introduction bitcoin
Purpose of a blockchain

- Ledger of who owns what
- Most examples centralized and require trusted party
  - Land registry: one database, we trust the government
  - Bank account: one database, we trust the bank
- Decentralized and without trust
  - keep all ledgers synchronized
  - Everybody has an incentive to fake the ledger
  - Who’s ledger is correct?
  - Cannot use voting as people can create fake identities?
- Bitcoin solves this problem
Idea behind a (Bitcoin) blockchain

- Blockchain is just a sequence of transactions
- Need to work through all transactions to find out balances (i.e. who has how many BTC)
- Easy to verify that “Charles gives 5 BTC to Alice” is an invalid transaction and should not be added
- Transactions are grouped in blocks

Alice gets 10 BTC
Alice gives 2 BTC to Bob
Bob gives 1 BTC to Charles
Charles gives 0.5 BTC Alice
Bob gives 0.5 BTC to Diana
Falsification problems

- I could go back and change the content of a block
- There is no central “true” ledger.
- I could claim my ledger is the correct one
- “Consensus” would be lost
- Many ledgers would emerge
- Nobody would trust this mechanism
- System would fail
Cryptographic Hash function

- Maps input of any length to an output of defined length (in our case 256 bit)
  \[ x \rightarrow h=H(x) \]

- Hash function is open source
- Easy to compute in one direction
- Computationally impossible to invert
  - Cannot find an input \( x \) if I only know the hash value \( h \)

- Hash function is like a checksum of some content
Idea behind a (Bitcoin) blockchain

- Each block has a hash value of its content to make it falsification proof
- Everybody can verify the integrity of a block
- The hash value of block 1 is included in computing the hash value of block 2
- All blocks are linked together

Alice gets 10 BTC
Alice gives 2 BTC to Bob
Bob gives 1 BTC to Charles
Hash value Block 1

Hash value block 1
Alice gives 0.5 BTC to Diana
Charles gives 0.5 BTC to Bob
Hash value Block 2
Falsification problem

- Hash values link blocks together in a clear sequence
- Altering a value will change the Hash value of block and would be detected
- It would be easy to verify that the block was tampered with

Alice gets 10 BTC
Alice gives 2 BTC to Alfred
Bob gives 1 BTC to Charles
Hash value Block 1

Hash value block 1
Alice gives 0.5 BTC to Diana
Charles gives 0.5 BTC to Bob
Hash value Block 2
Falsification problem

- Recompute hash value for block 1
- Now Block 1 is internally consistent (a valid block)
- But the new hash value does not match the first line of block 2
- It would be obvious that somebody tampered with block 1

Alice gets 10 BTC
Alice gives 2 BTC to Alfred
Bob gives 1 BTC to Charles
Hash value Block 1

Hash value block 1
Alice gives 0.5 BTC to Diana
Charles gives 0.5 BTC to Bob
Hash value Block 2
Falsification problem

The adversary has to also re-write block 2 to make block 1 and 2 link together

- Do this for all subsequent blocks
- If re-writing blocks was easy one could still fake the ledger
- Composing a block has to be made hard (computationally expensive)

Alice gets 10 BTC
Alice gives 2 BTC to Alfred
Bob gives 1 BTC to Charles
Hash value Block 1

Hash value block 1
Alice gives 0.5 BTC to Diana
Charles gives 0.5 BTC to Bob
Hash value Block 2
Mining

- Computing a block designed to be time consuming
- Re-computing all blocks is time consuming and costs resources (hardware, energy)
- While the adversary recomputes the blocks new blocks get added
- Ideally adversary can never catch up
- Making it hard to compute blocks is essential part of the blockchain mechanism
  - This reduces chances of falsification
Blocks are only valid when the hash value has a certain number of leading zeros

- Only works by trial and error
- Miners can change the composition of transactions and the block’s Nonce value (free to choose number)
- Difficulty is calibrated to get 1 block about every 10 minutes
Suppose that Alice wants to send 1 BTC to Bob

Bitcoin is a peer-to-peer network

Alice’s computer is in touch with other nodes on the bitcoin network. A node
  — keeps a copy of the whole blockchain
  — Relays new blocks and pending transactions

Alice’s computer creates a transaction and this gets floated to other nodes. It is in the memory pool.

Miners pick transactions out of the mempool to add to the block
Figure 8. Histogram of time between blocks with blockheight larger than 100,000, capped at 50 minutes.

Source: Lehar, Parlour, 2021, Miner Collusion and the BitCoin Protocol
Antminer S9

Deployed in late 2016, this was the flagship miner until not long ago. The miner is sold by Bitmain, and it usually ships in batches. If you can’t find available inventory, you can always look on eBay and get a new or used one (you’re protected by eBay’s money-back guarantee policy). The miner can reach 14 TH/s, but isn’t as efficient as the latest competition.

Manufacturer: Halong Mining

Power consumption: 1480W

Hash rate: 16 TH/s

Efficiency: 0.0925 j/GH

Chip process: 10 nm

Noise level: 75 db

Overall rating: ★★★★★

View sellers

DragonMint T1

Manufacturer: Bitmain

Power consumption: 1350W

Hash rate: 14.5 TH/s

Efficiency: 0.093 j/GH

Chip process: 16 nm

Noise level: 76 db

Overall rating: ★★★★☆

View sellers

Antminer S9

Manufacturer: Canaan

Power consumption: 1290W

Hash rate: 13.6 TH/s

Efficiency: 0.099 j/GH

Chip process: 16 nm

Noise level: 65 db

Overall rating: ★★★★★☆

View sellers

AvalonMiner 841

View sellers

Most ASICs look pretty much the same: like a rectangle box with a fan attached.

A Mining Facility
Hash Rate

156.0 EH/s

Kilo Mega Giga Tera Peta Exa

blockchain.com/charts
Problems with bitcoin

- **Deflationary:**
  - Numbers of bitcoin ever to be issued is capped

- **Environment**
  - Bitcoin network uses more electricity than Ireland or Norway
  - One transaction comparable to 1 household-1 month

- **Control of mining power**
  - Miners form pools to engage in risk sharing
  - Pools can get very powerful
Bitcoin problems

- Visa-problem: capacity of BTC too low
  - Visa processes 150m TX/day, can do >24000/sec
  - Feb 15, 2021: BTC has 296388 TX/day
  - Every node has to store all past transactions
    - BTC size Feb 2021: 317 GB
  - If you want your own wallet you have to run a node or trust another node (i.e. fully trust like a bank)

- Security costs borne by users
How to buy Bitcoin

- **Exchanges**
  - Allow you to trade Bitcoin and other crypto against Fiat (CAD, USD)
- **Paypal, other services**
- **Who has custody?**
  - As far as the blockchain is concerned the exchange owns the BTC
    - Exchange has internal ledger that attributes bitcoin to user
- **Problem when the exchange defaults**
  - All your money is lost
  - Completely unregulated
Crypto Exchange CEO Dies With Passcodes to Unlock Customers’ $199 Million USD

A strange twist for the scandalous firm.

How Weird Is It That a Company Lost Hundreds of Millions in Cryptocurrency Because Its CEO Died?

And is it more or less weird than customers’ allegation that the CEO faked his own death?

BY AARON MAK

Dec 18, 2019 • 5:02 PM

EY research finds cases of QuadrigaCX CEO using customer funds for crypto margin trading

by Giorgi Mikheilize — June 29, 2019 • In: Scam News • 1 min read

The CEO of Quadriga kept all of the encryption keys on a single laptop. AFP PHOTO / JACK GUEZ

JACK GUEZ/AFP
Keep with exchange
  — Need to trust exchange, no recovery in case of default

Keep in your own wallet
  — If private key is lost, your crypto is lost
  — Software Wallet
    ▪ Software on your computer/phone
    ▪ Most malware searches computers for wallet keys
  — Hardware wallet
    ▪ Connects to USB port
    ▪ Stores private key in device
Doing more with blockchain

- Instead of transaction data (Alice sends 1 BTC to BOB) store some other data on blockchain
- Other data can be anything (e.g. picture of Nelson Mandela)
- Data can be another ledger or computer program
- Create tokens
- A token is a digital item that can be owned and transferred
- Many run on Ethereum blockchain
Stablecoins
Privately issued money

- Stable coins are tied to the value of a fiat currency, e.g. USD
- Value can move up and down a bit but in general stable coins are stable
- Issued by private entities
- Use-cases
  - Crypto trading
  - Making payments: can send USD cheap to another part of the world
  - Settlement of smart contracts
  - Can get USD exposure outside of the US
### Stablecoin Statistics

<table>
<thead>
<tr>
<th>Name</th>
<th>Price (USD)</th>
<th>Market Cap</th>
<th>24h Volume</th>
<th>24h On-Chain Vol</th>
<th>24h On-Chain Txs</th>
<th>Blockchains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tether USDT</td>
<td>$1.00034</td>
<td>$32,422,105,701.19</td>
<td>$102,491,820,688.00</td>
<td>$3,565,844,872.40</td>
<td>121,961</td>
<td>🟩</td>
</tr>
<tr>
<td>USD Coin</td>
<td>$0.99976</td>
<td>$7,441,027,221.40</td>
<td>$2,058,912,097.00</td>
<td>$3,143,098,962.03</td>
<td>51,018</td>
<td>🟧</td>
</tr>
<tr>
<td>Multi-collateral DAI</td>
<td>$0.99759</td>
<td>$2,171,219,616.14</td>
<td>$374,110,175.00</td>
<td>$2,441,700,841.19</td>
<td>15,929</td>
<td>🟩</td>
</tr>
<tr>
<td>Binance USD</td>
<td>$1.00015</td>
<td>$1,585,445,957.08</td>
<td>$3,841,302,504.00</td>
<td>$812,850,074.86</td>
<td>1,635</td>
<td>🟩</td>
</tr>
<tr>
<td>sUSD</td>
<td>$4.63534</td>
<td>$1,374,683,476.16</td>
<td>$25,797,205.00</td>
<td>$804,426,830.71</td>
<td>2,611</td>
<td>🟩</td>
</tr>
<tr>
<td>Paxos Standard</td>
<td>$1.00034</td>
<td>$703,952,821.88</td>
<td>$136,640,927.00</td>
<td>$118,421,692.48</td>
<td>893</td>
<td>🟩</td>
</tr>
<tr>
<td>HUSD</td>
<td>$1.00042</td>
<td>$494,128,653.84</td>
<td>$119,672,616.00</td>
<td>$169,281,190.92</td>
<td>564</td>
<td>🟩</td>
</tr>
<tr>
<td>TrueUSD</td>
<td>$1.00011</td>
<td>$329,342,863.37</td>
<td>$151,427,876.00</td>
<td>$167,058,505.16</td>
<td>1,933</td>
<td>🟩</td>
</tr>
<tr>
<td>PAX Gold</td>
<td>$1,805.00000</td>
<td>$125,807,635.40</td>
<td>$8,486,272.00</td>
<td>$9,501,161.90</td>
<td>643</td>
<td>🟩</td>
</tr>
<tr>
<td>Gemini Dollar</td>
<td>$1.01314</td>
<td>$110,453,412.55</td>
<td>$5,514,804.00</td>
<td>$65,391,496.20</td>
<td>920</td>
<td>🟩</td>
</tr>
</tbody>
</table>
Arbitrage with Tether treasury keeps price stable
  — Allow conversion between USDT and US-Fiat
Types of stable coins

- Asset backed off chain
  - Fiat backed e.g. USDT, USD Coin
  - Commodity backed: often gold
  - Audited/not audited
  - Hold fiat in insured banks or not

- Asset backed on chain
  - Use other cryptos as collateral: e.g. Maker, Dai
  - Collateral value visible (on chain)

- Usage fees
Private money

- In Hong Kong paper bills are issued by private banks (upon the authority of the central bank - HKMA)
- In periods of free banking private banks issued “bank notes”: Canada, US, Great Britain, Switzerland, China, many other countries
  - Bank notes denominated in local currency, e.g. USD
  - In good times notes were interchangeable
  - Clearing houses took care of situations when somebody presented a bill issued by one bank to deposit in another
  - When a bank is fragile its notes might not be accepted
  - System is fragile
  - Contagion might spread to other banks
  - Main reason for monopoly central banks
Can stablecoins be a source of financial instability?

- How do stablecoin issuers make money?
- Issue non-interest bearing coins for USD
- Invest proceeds into financial markets and earn interest
- Short term, liquid investments (e.g. bank deposits) do not create high returns
- Temptation to invest in longer term instruments for higher returns
- Generates liquidity risk
  - If all stablecoin users want to convert to fiat there is not enough liquid cash
  - Fire sale of illiquid assets causes price to drop -> not enough to cover issued stable coins
Financial fragility

Assume users redeem 30 stable coins
20 can be paid back from liquid assets
Need to sell 10 units of the bond. Then price drops to 90 → need to sell more bonds → price drops more
Outcome might be like this

- Insufficient funds to cover existing coins
- Everybody else anticipates this and redeems

<table>
<thead>
<tr>
<th>Liquid Assets</th>
<th>Stablecoins</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>85 illiquid</td>
<td></td>
</tr>
<tr>
<td>(85 bonds at price 100)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liquid Assets</th>
<th>Stablecoins</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>70</td>
</tr>
<tr>
<td>61.6 illiquid</td>
<td></td>
</tr>
<tr>
<td>(70 bonds at price 88)</td>
<td></td>
</tr>
</tbody>
</table>
This problem is not new

Main problem of banking
- Long term illiquid loans
- Liquid short term deposits

Solutions
- Government deposit insurance
  - Not likely for stablecoins
- Strict liquidity regulation and extra capital requirements
  - Costly for issuer, hard to enforce
- Credibility of regulator
  - Watch out for own citizens first
Stablecoin Limitations

- **Regulatory**
  - Stablecoins might violate securities law in most countries

- **Centralization**
  - Run by few corporations. Trust is required
  - Why trust Tether more than CIBC?

- **Security**
  - A run could also happen due to a hack
• Stablecoin proposed by Facebook
• Use basket of global currencies as collateral
• Trusted set of verifiers (limited number of companies)
• Same problems as with other stablecoins
• Can Facebook block your access to this market?
  — What if you are a critic of Zuckerberg?
• Can the US government freeze your coins?
• Privacy on transactions?
• Know your customer (KYC) and Anti Money Laundering (AML) enforcement?
- How do smart contracts work?
- Will the Bank of Canada issue a crypto loonie?
- Decentralized finance
- Yield Farming: investing your crypto