NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural

Department of Computer Science & Engineering

Indian Institute of Technology Kharagpur

Lecture 17: Blockchain Elements - V

CONCEPTS COVERED

- Start of the Bitcoin Network and Creation of Coins
- Variation of Block Reward with Time
- Handling of Double Spending Problem
- Payment using Bitcoin and Anonymity
- Bitcoin Exchange

KEYWORDS

- Block Reward
- Double Spending
- Anonymity
- Bitcoin Exchange

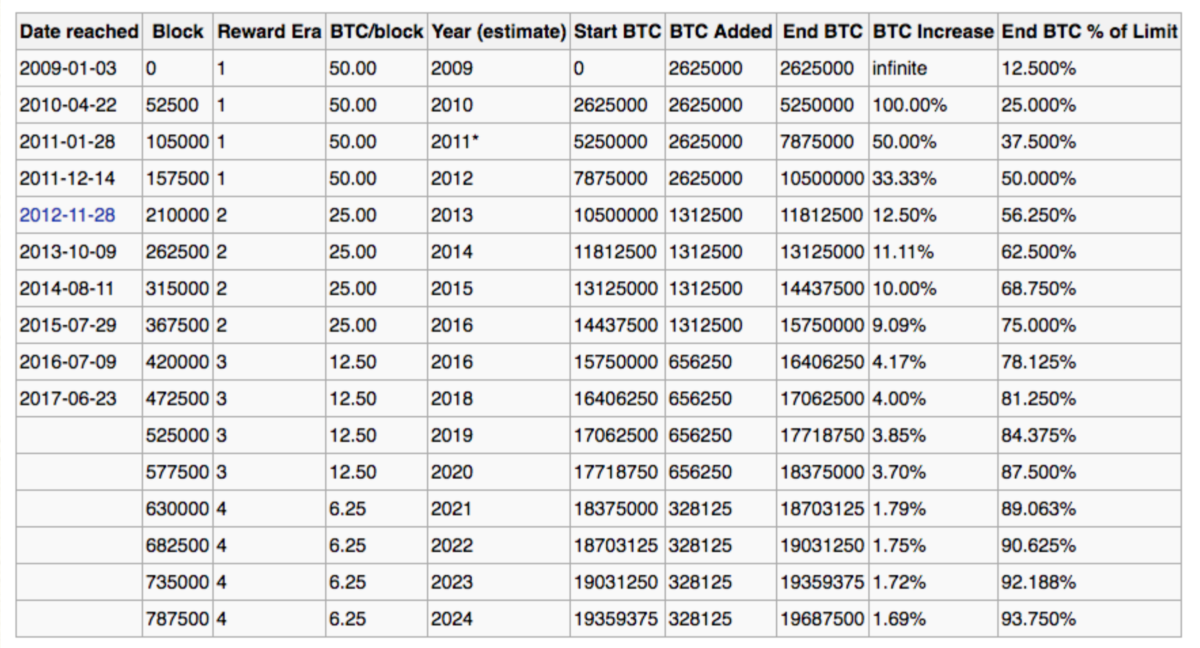
Bitcoin Basics – Creation of Coins

- **Controlled Supply:** Must be limited for the currency to have value – any maliciously generated currency needs to be rejected by the network
- Bitcoins are generated **during the mining** – each time a user discovers a new block
- The rate of block creation is adjusted every 2016 blocks to aim for **a constant two week adjustment period**
- The last bitcoin will be mined in 2140 (estimated and unless changed)

Bitcoin Basics – Creation of Coins

- Number of bitcoins generated per block is set to decrease **geometrically**, with a 50% reduction for every 210,000 blocks, or approximately 4 years
- This reduces with time the amount of bitcoins generated per block
  - Theoretical limit for total bitcoins: Slightly less than *21 million*
  - Miners will get less reward as time progresses
  - How to pay the mining fee – increase the transaction fee

Projected Number of Bitcoins



Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	50.00%	37.500%
2011-12-14	157500	1	50.00	2012	7875000	2625000	10500000	33.33%	50.000%
2012-11-28	210000	2	25.00	2013	10500000	1312500	11812500	12.50%	56.250%
2013-10-09	262500	2	25.00	2014	11812500	1312500	13125000	11.11%	62.500%
2014-08-11	315000	2	25.00	2015	13125000	1312500	14437500	10.00%	68.750%
2015-07-29	367500	2	25.00	2016	14437500	1312500	15750000	9.09%	75.000%
2016-07-09	420000	3	12.50	2016	15750000	656250	16406250	4.17%	78.125%
2017-06-23	472500	3	12.50	2018	16406250	656250	17062500	4.00%	81.250%
	525000	3	12.50	2019	17062500	656250	17718750	3.85%	84.375%
	577500	3	12.50	2020	17718750	656250	18375000	3.70%	87.500%
	630000	4	6.25	2021	18375000	328125	18703125	1.79%	89.063%
	682500	4	6.25	2022	18703125	328125	19031250	1.75%	90.625%
	735000	4	6.25	2023	19031250	328125	19359375	1.72%	92.188%
	787500	4	6.25	2024	19359375	328125	19687500	1.69%	93.750%

Information Source: https://en.bitcoin.it/wiki/

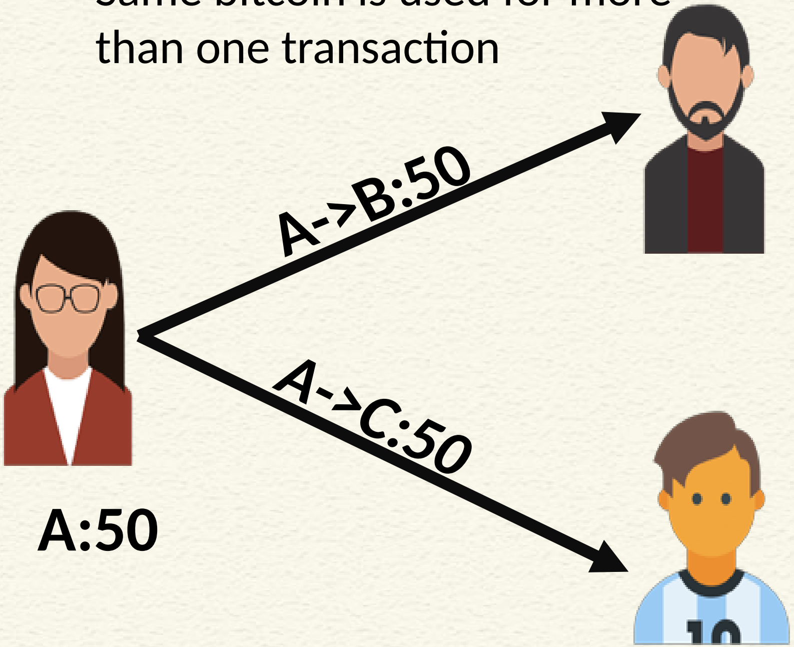
Bitcoin Basics – Sending Payments

- Alice wants to send bitcoin to Bob
  - Bob sends his address to Alice
  - Alice adds Bob's address and the amount of bitcoins to transfer in a "transaction" message
  - Alice signs the transaction with her private key, and announces her public key for signature verification
  - Alice broadcasts the transaction on the Bitcoin network for all to see

Information Source: https://en.bitcoin.it/wiki/

Double Spending

- Same bitcoin is used for more than one transaction



- Double spending Cash??
- In a centralized system for digital currency, the bank prevents double spending
- **How can we prevent double spending in a decentralized network?**

Handle Double Spending using Blockchain

- When multiple valid continuation to this chain appear, only the longest such branch is accepted and it is then extended further **(longest chain)**
- Once a transaction is committed in the blockchain, everyone in the network can validate all the transactions by using Alice’s public address
- The validation prevents double spending in bitcoin

Bitcoin Anonymity

- Bitcoin is permission-less, you do not need to setup any “account”, or required any e-mail address, user name or password to login to the wallet
- The public and the private keys do not need to be registered, the wallet can generate them for the users
- The **bitcoin address** is used for transaction, not the user name or identity

Bitcoin Anonymity

- A **bitcoin address** mathematically corresponds to a public key based on ECDSA – the digital signature algorithm used in bitcoin
- A sample bitcoin address: 1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz
- Each person can have many such addresses, each with its own balance
  - Difficult to know which person owns what amount

To Sum it All Up!!

- Bitcoins do not really “exist” as any tangible or electronic object.
- There is no bit”coin” as you see in its logo
- Owning a bitcoin simply means you have access to a key pair that includes
  - A public key to which somebody else had sent some bitcoin
  - A matching private key that gives you the authority to send the previously received bitcoin to another address
- If you lose your private key, you lose the corresponding bitcoin(s)

Physical Payment using Bitcoin

- All that is needed is a (set of) private key(s) – Public key can be generated from the private key.
- Safely store the private key – in your desktop, on the web, mobile phone, special hardware attachment, printed on a piece of paper as QR
- For online payment, you can use the wallet and an appropriate mode of applying the private key
- For off line payments like in store payments or paying to your friend, you can use your mobile phone to present the private key or use the hardcopy!! As simple as using PayTm, Google Pay and so on.

Bitcoin Exchange

- Trading bitcoin as commodity
- Centralized exchanges – (In India: WazirX, CoinDCX, Zebpay, CoinSwitch Kuber, etc.)
  - Identity verification using KYC documents
  - Maintain your balance in Bitcoin and another currency like INR.
  - You set the buying and selling prices and quantities
  - If necessary, you can take the money out in a referred currency
  - Some exchanges provide the payout option in anonymous prepaid cards
- There can also be decentralized exchanges with appropriate procedures for handling similar requirements

CONCLUSIONS

- Generation (Mining) of new coins
- Variation of block reward with time
- Handling double spending
- Anonymity in bitcoin
- Paying using bitcoin and role of exchange

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Hype or Innovation by Tatiana Gayvoronskaya and Christoph Meinel, Springer (2021)
- Any other standard textbook on blockchain/bitcoin

Thank you