**Lecture 9 Notes**

Slide 4

* “A **decentralized** digital currency enables instant payments to anyone, anywhere in the world”.

– en.bitcoin.it

* No central authority uses peer-to-peer technology.
* Two broad operations
  + **Transaction Management** – transfer of bitcoins from one user to another.
  + **Money Issuance** – regulate the monetary base.

Slide 5

* Node A and B will have key pair (public and private key).
* Node A and B are anonymous.
* Node A and B will be identified by the wallet address.
* Node A and B can also become the miner.
* Nodes can join the network anytime, anywhere around the world.

Slide 6

* Transaction get initiates between the users.
* Miners will collect the set of transactions and construct the block.
* Miners must solve the puzzle.
* Miner who solve the puzzle first will get chance of adding his block to the existing blockchain.
* Transaction will get verified by the miners and validated by validator nodes.
* Transaction gets executed.

Slide 7

* The 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 number 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

Slide 9

* Need to ensure that Eve cannot spend Alice’s bitcoins by creating transactions in her name.
* Bitcoin uses **public key cryptography** to make and verify digital signatures.
* Each person has one or more addresses each with an associated pair of public and private keys (may hold in the bitcoin wallet)

Slide 10

* Alice wish to transfer some bitcoin to Bob.
  + Alice can sign a transaction with her private key
  + Anyone can validate the transaction with Alice’s public key

Slide 11

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.

Slide 12

* Same bitcoin is used for more than one transaction
  + In a centralized system, the bank prevents double spending

Slide 13

* **How can we prevent double spending in a decentralized network?**
* Details about the transaction are sent and forwarded to all or as many other computers as possible.
* Use **Blockchain** – a constantly growing chain of blocks that contain a record of all transactions
* The blockchain is maintained by all peers in the Bitcoin network – everyone has a copy of the blockchain
* To be accepted in the chain, transaction blocks must be valid and must include **proof of work** – a computationally difficult hash generated by the mining procedure.
* Blockchain ensures that, if any of the block is modified, all following blocks will have to be recomputed.
* 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.

Slide 16

* Bitcoin is permission-less, you do not need to setup any “account”, or required any e-mail address, username, 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 username or identity.
* A **bitcoin address** mathematically corresponds to a public key based of 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.

Slide 17

* An ad-hoc network with random topology, Bitcoin protocol runs on TCP port 8333.
* All nodes (users) in the bitcoin network are treated equally.
* New nodes can join any time, non-responding nodes are removed after 3 hours.