Learning Blockchain
(Lecture#10 - 9 Sept 2019)

Dhiren Patel

VJTI Mumbai

Blockchain Basics (list)

- Keys
- Addresses
- Wallets
- Transactions
- Scripting
- Mining
- Consensus
- Forks

Consensus

- Proof of Work (Work – resource consumption)
- Proof of Stake (Stake – investment, trust)
- Validators - Majority – k out of n
- Delegated PoW / PoS
- Delegated Entities (Transaction Validators) – small number, selection, active time window, replacement mechanism, turn again, tweaking k out of N

Keys

- Digital keys not stored in the network, but are created and stored by users in a file (or database) called a wallet
- Properties:
- Decentralized trust
- Ownership attestation
- Cryptographic proof security model

Keys (cont)

- Digital signature – used to spend funds (witness) – testifies to the true ownership of the funds being spent
- Key comes in pair (Private key and Public key)
- Analogy: Bank account number or login ID, and secret PIN or password
- For the most part, these keys are stored inside the wallet and managed by wallet software

Private and Public keys

- Private keys
- a number between 1 and n-1 (where n is 2^{256})
- How to choose? - Take a string – input it to SHA256 – will give 256 bit output
- Public key – generated from private key using ECC (trap door multiplication)
- K = k*G where k = private key and G is generator point
- For Bitcoin – curve is secp256k1

Addresses

- E.g. Bitcoin address – string of digits and characters, starting digit 1, derived from Public key.
- Address = RIPEMD160(SHA256(Public key K))
- 160 bit - 20 bytes
- Base58Check 0x00 prefix = 1 in Base58
- Base58 = digits, upper case, lower case (without 0, O, l, I)
- Conversion to Base58Check format

Wallets

- UI (User Interface)
- Controls access to user’s currency, managing keys and addresses, tracking the balance, creating and signing transactions
- Wallet – essentially contains keys (bitcoin wallet is known as keychain)
- Users control the coins on the network.
- Non-deterministic (Random) wallets
- Deterministic (Seeded) wallets
- HD wallets (single seed)
- Mnemonic codes based (12 words) (BIP 39)

VJTI Blockchain

- Install from google play store dApp on Android phone
- Coins will be given later
- FDP/Officials training program – 30 Sept to 4 Oct 2019
- Registration on https://vjti-bct.in/fdp2019

Blockchain Analysis

- Process of inspecting, identifying, clustering, modelling and visually representing data on a blockchain
- Useful for discovering knowledge about actors transacting on the chain

Project based learning

- Learning by doing experimentations
- Mid-sem exam (20 Sept - Friday)
- Open notes (2 full scape sheets, hand written)
- Grace marks for (no notes)
- Survey#3 on mid-sem