COSC 5010 - Blockchain Design and Programming Lecture Note 1

Libao Jin (ljin1@uwyo.edu)

October 24, 2018

1 Hash function

Microsoft Windows using NTLM, NTLM4.

1.1 What is a hash?

A hash is a mapping from a range to a domain.

- Zero knowledge proof: SRP (SSH).
- Telegram: 2.1 billion (fund raising)
- Approvable identity
- Mineral rights
- DLL (Dynamic Linking Library)
- Fiduciary Responsibility
- artitrage simultaneous buy and sell commodity in different markets for different prices.

2 Mining

1. Serialize Block
2. Hash Bytes -> h
3. If h has "Property" then done.
4. Increment "Nonce"

- Proof of Authority/Stack
- Merkle Tree
- "Public Ledger"
- "Smart Contract": the program move the value from one to the other.
- "Non Fungable": ERC 721
- "Fungable": ERC-20

2.1 Cryptographic Hash

1. Deterministic
2. To fake requires all possible inputs
3. Small chnage in inputs would cause large change in output
4. Infeasible to find collisions

- Monera
- zCash

- Cash
- Stock - 100
- P & L
- Long on Cash
- Long on IBM
- Realestate Investing
- REIT
- Inflation
- Defaltion
- P/E ratio
- Dividends
- Yield: convert Dividends to Percentage...
- Derivative
- Bonds: $10,000 TBill, Discount Rate (annual), 210 BSP (Bias Points) = 2.1%.
- Asset Allocation
  - Average 12.2% Per Year Since October 31, 1929 (Great Depression).
  - Average 12.0% Per Year Since September 01, 1929 (Great Depression).
- Index Fund
  - 401K: $18400 -> $52K, $24800 -> $64K.
- Mutual Funds - Expense Ratio (2%)
- NAIC
- ICO (Initial Coin Offering): Register with SEC
  - Industrial Staker Sale
  - Consumer Token Sale
  - KNY - Know Your Investor (avoid money laundering)
- Proforma
- Prospectus

2.2 ICO

- HB-70 Public Traded LLL,
- ICO
- High-Speeding Trading
- Inverstment in Apartment

2.3 Financial of Software Companies

- Adobe - Monthly License
- Software as a Service - Amazon Web Services
- ERC-721: cryptokitties
- ERC-20
- ERC-958
- Nigeria: 10% Economy is based on blockchain.
- Raisin Capiptal ICO.
- Telegram: raise 4.3 billion capital.

2.4 Basics of Accounting

[]@ll@

Debit	Credit
Assets Draws	Liabilities Equity
Expenses	Reuinuse

2.5 How to Create Wealth

2.5.1 Startup

In Computer Science, $101,000…

- Leverage
  - Technology
    - Block Chain is the innovation in accouting in 5000 years.
- Measurement
- CEO, would make 300 times of average salary

2.5.2 Example

1. Loan $50,000

   []@ll@

	Debit	Credit
	$50000 Asset “Cash” Expense	Liability $50,000 Loan Cash $1,000
	$1,000 Rent Asset CNC $4,000	Cash $4,000 Cash $500 Reuniuse
	Draw $500 to Owner Cash $12,000	$12,000

2.5.3 Block Chain

- Crypto-currency
- Law
- Accounting
- Real Estate
- Finance ICO
- dApps Development

3 Class notes

- Go - "otto" - EcvnaScript/JavaScript - Build a blockchain
- Solidity Ethereum - web3.js, HTML, CSS and dApp
- Smart Contract

4 Technical Concepts

4.1 Merkle Tree

In cryptography and computer science, a *hash tree* or *Merkle tree* is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

4.2 Implementation of Wallet

```
$ ./main --create-genesis
$ ./main --list-accts
$ ./main --server 127.0.0.1:9000
$ cd pathTo/wallet-client
$ ./wallet-client --cmd accts
$ ./wallet-client --cmd list-accts (line 111, implementation)
```

4.3 HW 6

- Server
  - Listen
    - URL, `http://127.0.0.1:9000/opi/validate-signed-message`
- Client
  - `DoGet(URL, "acct", 0x44)`
  - Status code:
    - `200`: success.
    - `404`: not found.
    - `500`: interval server error.

4.4 Go Code for Test

1. Declare structure
2. Serialize - A structure: `tx/transaction.go`, `block/block.go`, `s := fmt.Sprintf("%10d: %s", iv, s)`
3. Hash - Call a hash function: `h := Keccak256([]byte)`
4. JSON - Read / Write
5. Map - Declare, Print
6. Declare function - Return values