

# Blockchain

Angelo Yang

# Blockchain

- Data Structure for Distributed Database
- Data Structure is a particular way of organizing and storing [data](#) in a computer so that it can be accessed and modified [efficiently](#).
- Bitcoin or Distributed Blockchain is not DS or AL, but blockchain is.

# Bitcoin

- Save digital currency(data) in secure and decentralized(efficiently) way.
- Why need to secure?
- Why need to decentralized?
- Secure and decentralized at the same time.

# Currency

- Early currency
- Coinage
- Paper money
- Banknote -> Transaction is solution!

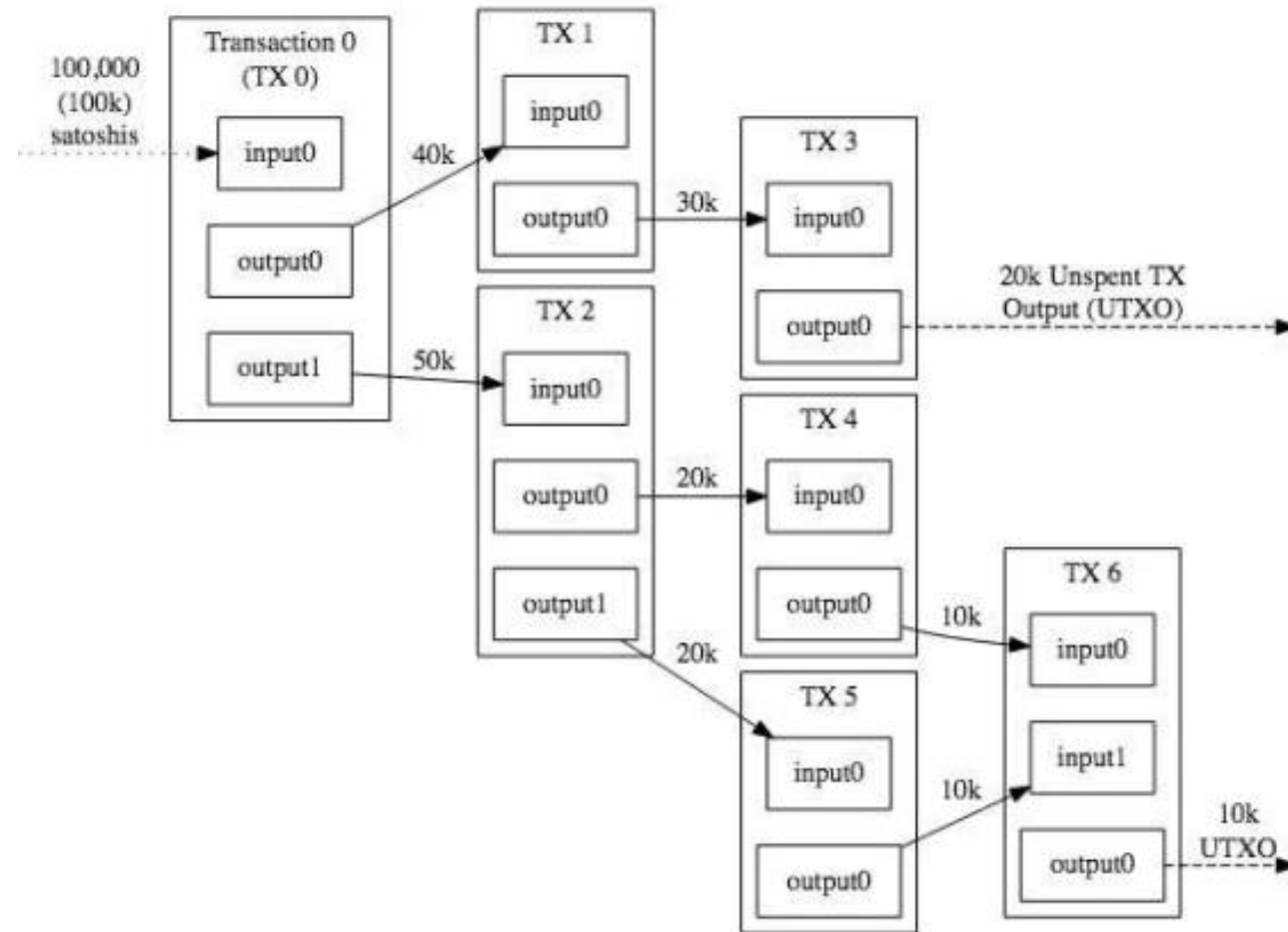
# Transaction

- Why transaction?... Nobody know.(Where I stuck everytime)
- It's just masterpiece of pre-era.
- Atomicity -> commit or rollback
- Consistency
- Isolation
- Durability -> Even crash after commit
- SQL(Structured Query Language)

# UTXOs(Unspent Transactions Outputs)

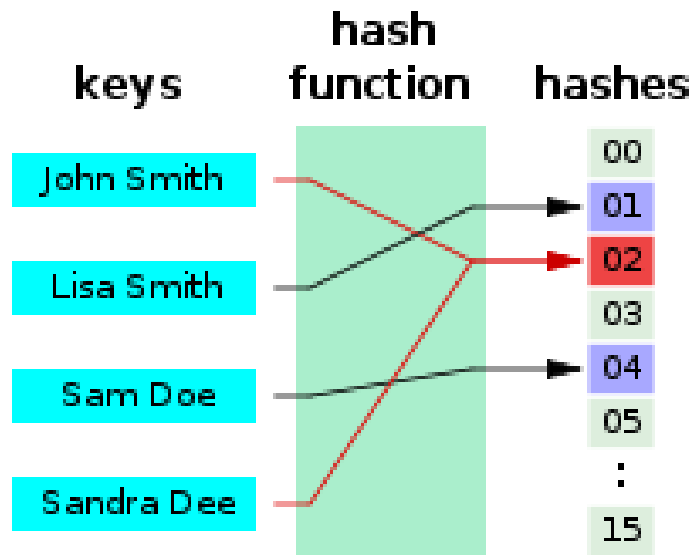
- Algorithm of Bitcoin
- Tx imply financial transaction
- Tx Format: (From)-(To)-(Value)
- I want to excute 'A-B-100'
- We just find and inherit '\*-A-\*' until sum of value more than 100

# UTXOs(Unspent Transactions Outputs)



# Hash

- We want to save transaction(digital currency) in secure and decentralized way.
- Hash is solution for security.





# Distributed Blockchain

- We want to save transaction(digital currency) in secure and decentralized way.
- Distributed Blockchain is solution of decentralizing.

# Distributed Blockchain

- Block = Nonce + Data
- Nonce is the random key which makes output of hash following specific rule => Proof of work

Block: # 1

Nonce: 10

Data: hi

Hash: 8c28724f6e93be2b70e6dff2cdefc081f6b96cca1e60f94de9fa4bf3639f6c1

Mine



Block: # 1

Nonce: 59396

Data: hi

Hash: 0000d742711b9c79c3464eaacdfa0153206221aedd749612b48f22475a96f912

Mine

# Distributed Blockchain

- Data include hash value of previous block

[illegible]

Block:

#

2

Nonce:

35230

Data:

Prev:

000015783b764259d382017d91a36d206d0f

Hash:


000012fa9b916eb9078f8d98a7864e697ae83

Mine

Block:	# 3
Nonce:	12937
Data:	
Prev:	000012fa9b916eb9078f8d9
Hash:	0000b9015ce2a08b61216b
<div>Mine</div>	

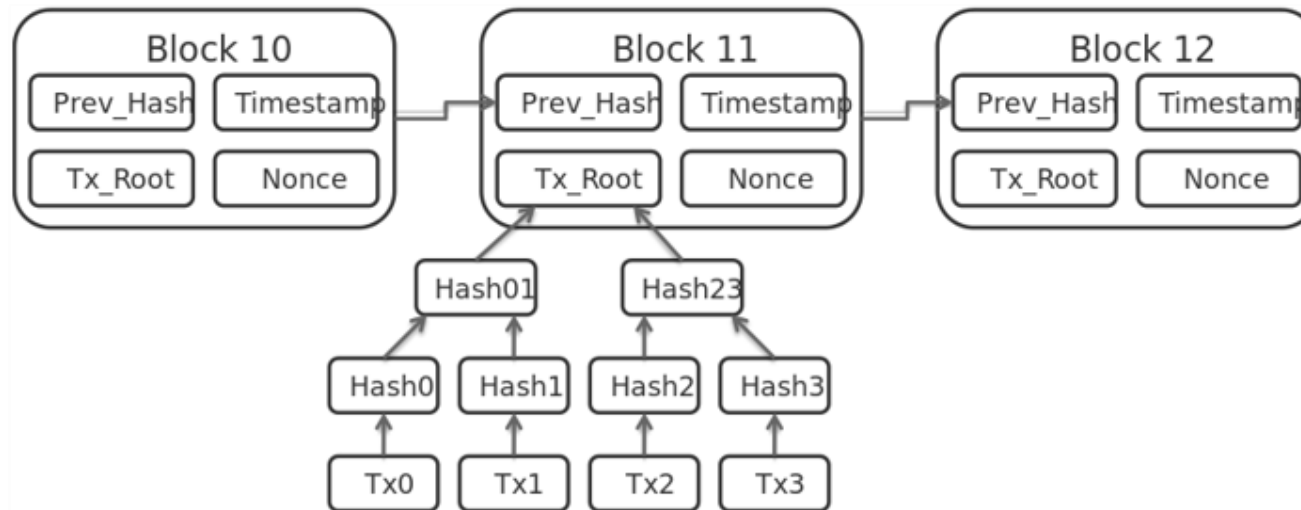
# Distributed Blockchain

- Data include hash value of previous block
- Data include Coinbase and Tx(s)(from requested Tx-set)

<div>Block: # 1</div> <div>Nonce: 16651</div> <div>Coinbase: \$ 100.00 -&gt; Anders</div> <div>Tx: </div> <div>Prev: 00000000000000000000000000000000</div> <div>Hash: 0000438d7625b86a6f366545b1929975a0d3</div> <div>Mine</div>	<div>Block: # 2</div> <div>Nonce: 37284</div> <div>Coinbase: \$ 100.00 -&gt; Anders</div> <div>Tx:<table><tr><td>\$ 10.00</td><td>From: Ande</td><td>-&gt;</td><td>Sophi</td></tr><tr><td>\$ 20.00</td><td>From: Ande</td><td>-&gt;</td><td>Lucas</td></tr><tr><td>\$ 15.00</td><td>From: Ande</td><td>-&gt;</td><td>Emily</td></tr><tr><td>\$ 15.00</td><td>From: Ande</td><td>-&gt;</td><td>Madis</td></tr></table></div> <div>Prev: 0000438d7625b86a6f366545b1929975a0d3</div> <div>Hash: 0000a5a24dd8f977c06df9f4c6e333cc0d37f6</div> <div>Mine</div>	\$ 10.00	From: Ande	->	Sophi	\$ 20.00	From: Ande	->	Lucas	\$ 15.00	From: Ande	->	Emily	\$ 15.00	From: Ande	->	Madis	<div>Block: # 3</div> <div>Nonce: 74806</div> <div>Coinbase: \$ 100.00 -&gt;</div> <div>Tx:<table><tr><td>\$ 3.14</td><td>From: Sylv</td></tr><tr><td>\$ 2.12</td><td>From: Twe</td></tr><tr><td>\$ 1.99</td><td>From: Daf</td></tr></table></div> <div>Prev: 0000a5a24dd8f977c06df9f</div> <div>Hash: 000057a728d2dc10eff73f1</div> <div>Mine</div>	\$ 3.14	From: Sylv	\$ 2.12	From: Twe	\$ 1.99	From: Daf
\$ 10.00	From: Ande	->	Sophi																					
\$ 20.00	From: Ande	->	Lucas																					
\$ 15.00	From: Ande	->	Emily																					
\$ 15.00	From: Ande	->	Madis																					
\$ 3.14	From: Sylv																							
\$ 2.12	From: Twe																							
\$ 1.99	From: Daf																							

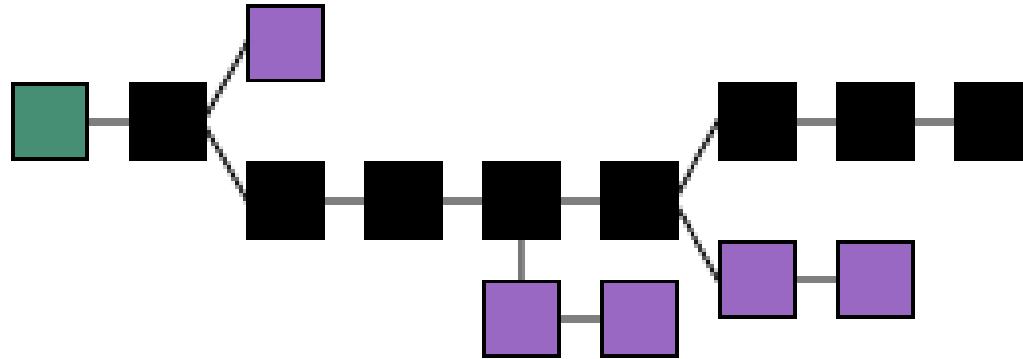
# Distributed Blockchain

- Actually, it's more complicated



# Distributed Blockchain

- Bitcoin choose race.
- Stability = the longest chain is valid chain
- Result slow transaction



# Bitcoin's Main Problem

- Race make un-decentralized, slow transaction
  - Limit of Bitcoin, first implementation of blockchain
- Size of full node
  - Metachain
  - Pruning
- 51% attack
  - Basic principle of cryptology
  - What if other blockchain which has other data?
    - Personal value or virtue
    - Memory of human network
- We'll find masterpiece of blockchain.

# Reference

- [https://en.wikipedia.org/wiki/Data\\_structure](https://en.wikipedia.org/wiki/Data_structure)
- <https://en.wikipedia.org/wiki/Blockchain>
- <https://en.wikipedia.org/wiki/Currency>
- <https://en.wikipedia.org/wiki/Banknote>
- <https://en.wikipedia.org/wiki/Coin>
- [https://youtu.be/\\_160oMzblY8](https://youtu.be/_160oMzblY8)