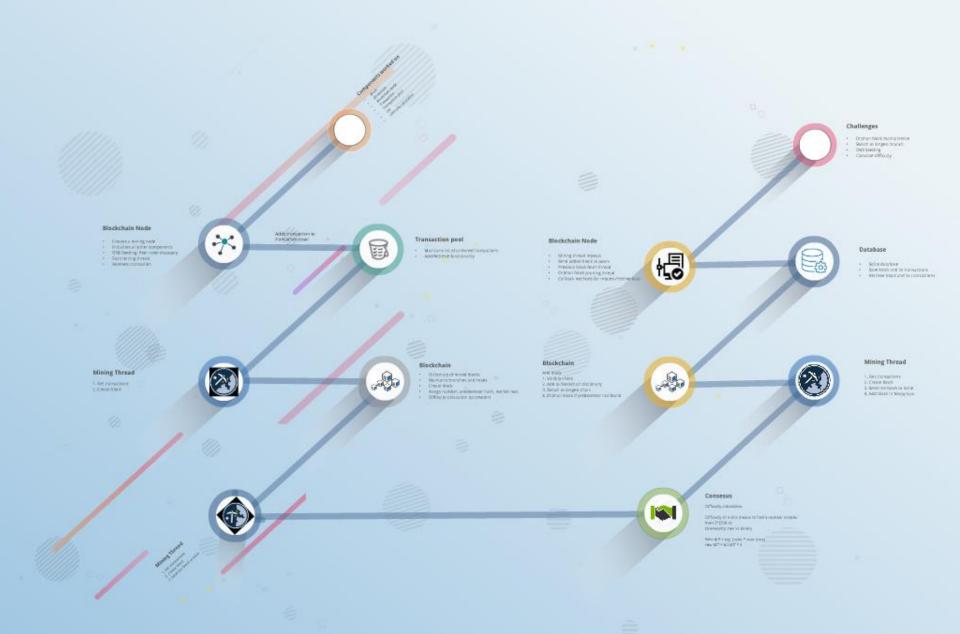# Labchain
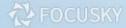
Farhad Ali
Owais Ahmed
Nishit Gajjar
Saurav Das
Siddharth Mehrotra
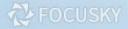
Components worked on

Challenges
- Orphan block must be done
- Switch to longest branch
- DNS Seeding
- Calculate difficulty

Blockchain Node
- Creates a mining node
- Initializes all other components
- DNS Seeding: Peer node discovery
- Start mining thread
- Generate transaction

Adds transaction to transaction pool

Transaction pool
- Maintains list of unverified transactions
- Add/remove & necessity

Blockchain Node
- Mining thread: impacts
- Send added block to peers
- Previous block fetch thread
- Orphan block pre-ring thread
- Callback methods for request/receive data

Database
- Solve database
- Save block and its transactions
- Retrieve block and its transactions

Mining Thread
1. Add transactions
2. Create block

Blockchain
- Dictionary of mined blocks
- Maintains branches and heads
- Create block
- Assign number, predecessor hash, merkle root
- Diffing proof-of-work parameters

Blockchain
Add block
1. Validate block
2. Add to blockchain dictionary
3. Switch to longest chain
4. Orphan block if predecessor not found

Mining Thread
1. Get transactions
2. Create block
3. Send the block to mine
4. Add block to blockchain

Mining Thread
1. Get transactions
2. Create block
3. Create the block and mine

Consesus
Difficulty calculation

Difficulty of a block means to find a number smaller than 2^256 in:
Developing chain vs binary

$new\ diff = log_2(old) * max\ tries$
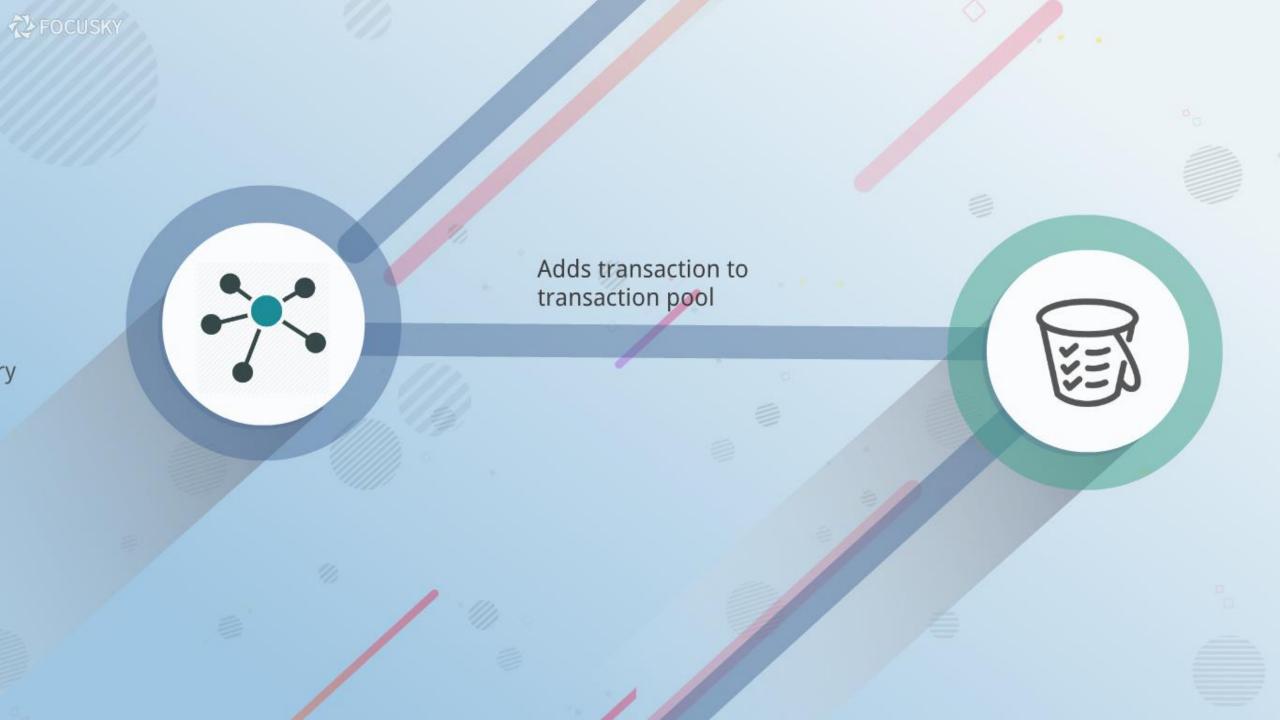$new\ diff = avg\ diff * t$

Components worked on

- Block
- Blockchain
- Blockchain Node
- Transaction
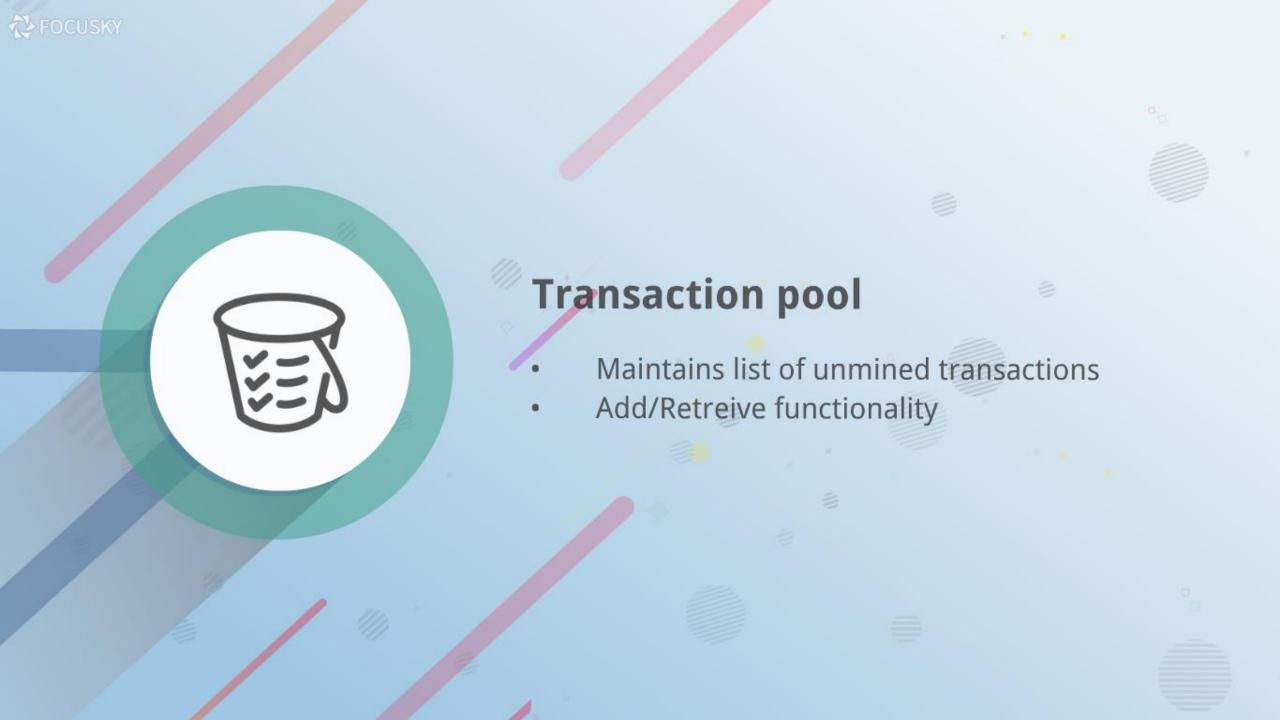- Transaction pool
- DB
- Difficulty calculation

Blockchain Node

- Creates a mining node
- Initializes all other components
- DNS Seeding: Peer node discovery
- Start mining thread
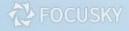- Receives transaction

Adds transaction to
transaction pool

Transaction pool

- Maintains list of unmined transactions
- Add/Retreive functionality

Mining Thread

1. Get transactions
2. Create block

Blockchain

- Dictionary of mined blocks
- Maintains branches and heads
- Create block
- Assign number, predecessor hash, merkle root
- Difficulty calculation parameters

Mining Thread

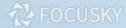1. Get transactions
2. Create block
3. Send the block to mine

Consesus

Difficulty calculation

Difficulty of n-bits means to find a number smaller than $2^{(256-n)}$
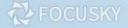Granularity: hex vs binary

New diff = log (ratio * max tries)
Hex diff = bit diff * 4

2

Mining Thread

1. Get transactions
2. Create block
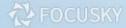3. Send the block to mine
4. Add block in blockchain

Blockchain

Add block

1. Validity check

2. Add to blockchain dictionary

3. Switch to longest chain

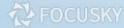4. Orphan block if predecessor not found

Database

- Sqlite database
- Save block and its transactions
- Retrieve block and its transactions

Blockchain Node

- Mining thread repeats
- Send added block to peers
- Previous block fetch thread
- Orphan block pruning thread
- Callback methods for request/receive data

Challenges

- Orphan block maintainence
- Switch to longest branch
- DNS Seeding
- Calculate difficulty