CS6290 Group Project

Conflux Protocol: Study, Test, and Implementation

Group 7

LING Shengchen, HE Jingrao, and ZHAI Liuqun

April 13, 2023

Contents

- **Part 1: Study the papers of Conflux protocol.**
- **Part 2: Study the new features after hard fork.**
- **Part 3: Test basic operations on official Testnet.**
- **Part 4: Run an independent chain and analyze.**

Blockchain Performance Problem

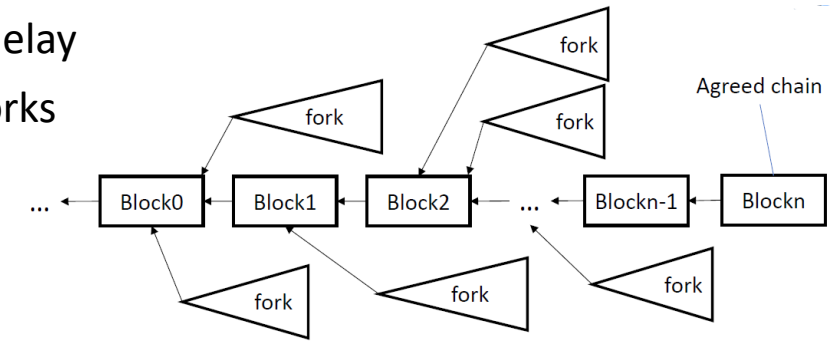
- **Ideal Blockchain System**
  - Robust against different attacks (double spending, DoS)
  - High Performance (high throughput, fast confirmation)
  - Decentralization
- **Real Blockchain & Payment System**

Transactions per Second	~7	~30	~200	~3000
Confirmation Latency	1 hour	7-10 minutes	Few seconds	Few seconds

Undesirable user experience!

Standard Nakamoto Consensus

- **Longest-chain**: all participants agree on the longest chain as the valid transaction history
- **Slow/small** block generation
  - Bitcoin: 1MB block per 10 minutes
  - Ethereum: ~100KB block per 15 seconds
- Run Nakamoto Consensus with large blocks or fast generation
  - Mining are concurrent and block broadcast has delay
  - Larger block size/faster block-gen rate -> more forks
  - Forks waste network/processing resources
  - Downgrade safety



GHOST and Structured GHOST

- **GHOST Consensus**
  - Heaviest subtree rule
  - Start from the Genesis block
  - Iteratively advance to the child block with the largest subtree

Suffers from liveness attack!

- **Structured GHOST Consensus**
  - Only **1/h** of blocks have weights for chain selection
  - Secure against liveness attacks if **h** is large enough
  - Need to wait for enough weighted blocks being generated to confirm

Slow confirmation!

How to keep fast confirmation under attacks?

Part 1: About Conflux

- **Conflux Network**: a scalable and decentralized blockchain system with high throughput and fast confirmation.

- **Greedy Heaviest Adaptive SubTree (GHAST):** combine original GHOST and structure GHOST.

- **Tree-Graph ledger structure (DAG):** a novel consensus protocol which optimistically processes concurrent blocks without discarding any as forks.

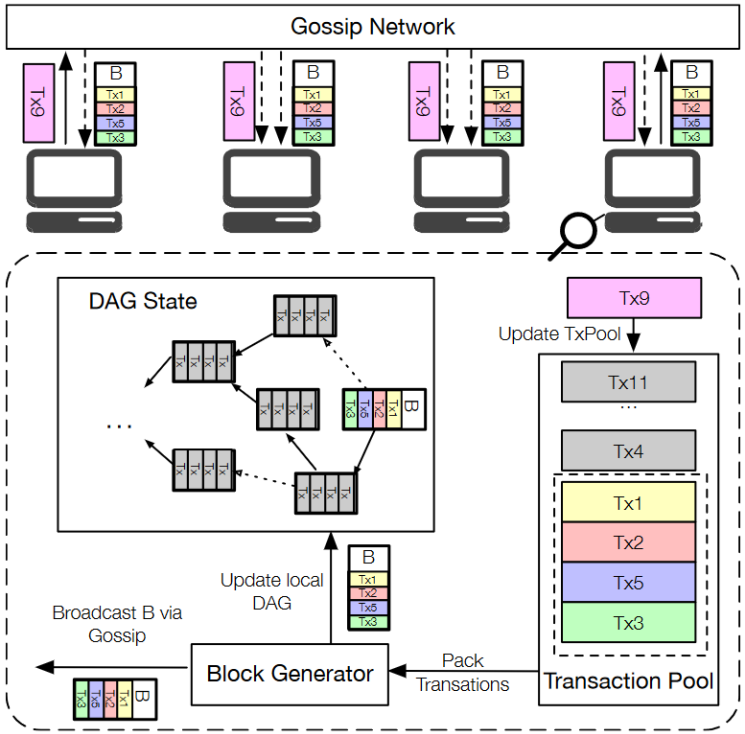


Fig. 1 Architecture of Conflux

Greedy Heaviest Adaptive SubTree (GHAST)

- Assign different weights to generated blocks
- Select Pivot Chain using heaviest subtree rule and decide total order of all blocks based on the pivot chain.

Assign equal weights to all blocks (GHOST)

+

Assign high weights to a small subset of blocks (structured GHOST)

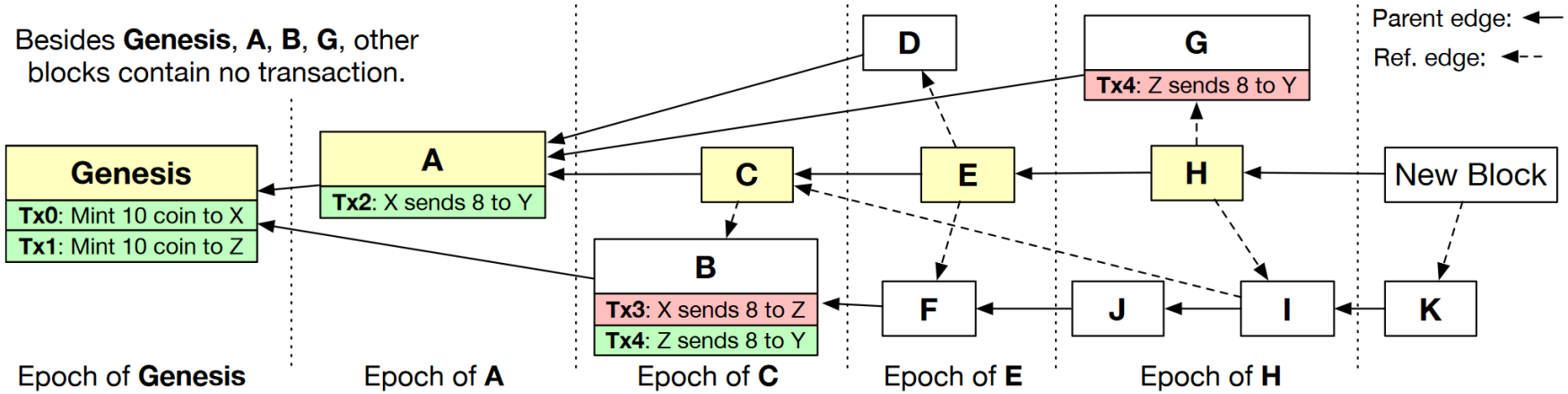
Normal scenarios

- Achieve near optimal throughput and confirmation latency

When attacks happen

- Slow confirmation to ensure consensus progress

Part 1: Tree-Graph structure of Conflux



Edges of one block

- Each block has one parent edge.
- Each block may have multiple reference edges. -- denote happens-before relationships.

When generating a new block,

- Select the last block in the pivot chain as the parent.
- Create reference edges to all other blocks without incoming edges.

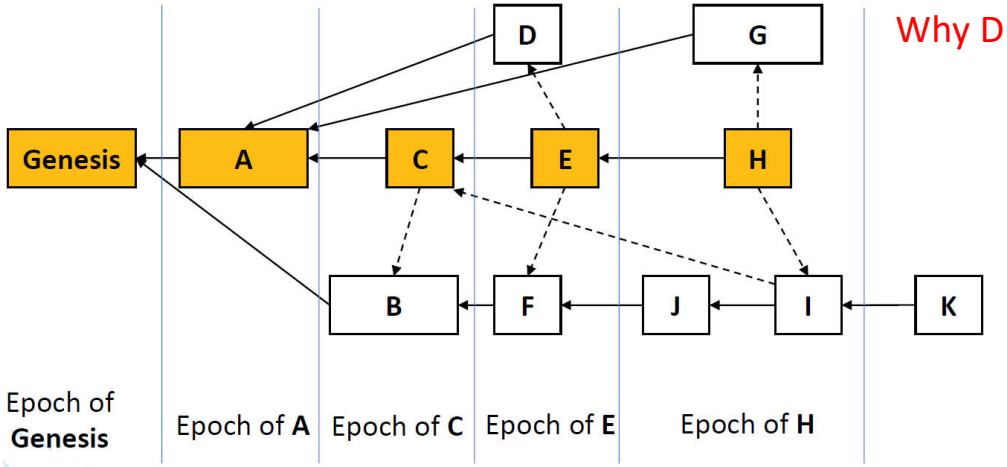
Part 1: Conflux Block Ordering

Key idea of block ordering

- Define a block total order of a Tree-Graph based on the Pivot chain.

Steps for block ordering

- Use GHAST to agree on a pivot chain of blocks - Each pivot chain block forms one epoch
- Then extend the agreed pivot chain into a total order of all blocks in the Tree-Graph



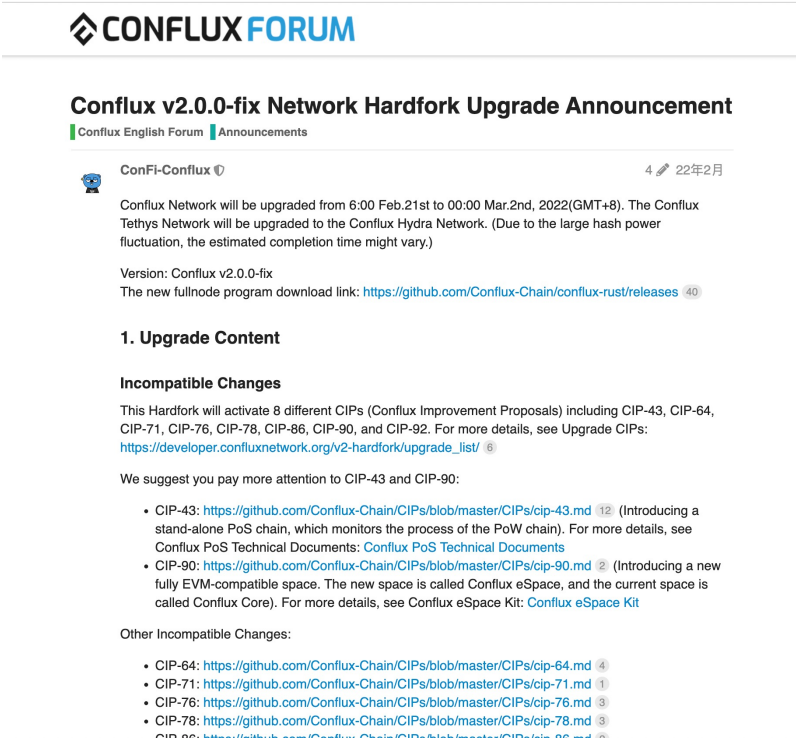
Why D belongs to the epoch of E?

- Order based on epoch first
- Topologically sort blocks in each epoch
- Break ties based on block id

Block Total Order: Genesis, A, B, C, D, F, E, G, J, I, H, K

Part 2: Study new features after hard fork

- **Conflux v2.0.0 hard fork**
  - in February 2022
  - CIP-43: Introduce PoS finality.
  - CIP-90: Introduce EVM compatibility.
  - And CIP-64, CIP-71, CIP-76, CIP-78, CIP-86, CIP-92.



CONFLUX FORUM

Conflux v2.0.0-fix Network Hardfork Upgrade Announcement

Conflux English Forum | Announcements

ConFi-Conflux 4 22年2月

Conflux Network will be upgraded from 6:00 Feb.21st to 00:00 Mar.2nd, 2022(GMT+8). The Conflux Tethys Network will be upgraded to the Conflux Hydra Network. (Due to the large hash power fluctuation, the estimated completion time might vary.)

Version: Conflux v2.0.0-fix
The new fullnode program download link: https://github.com/Conflux-Chain/conflux-rust/releases 40

1. Upgrade Content

Incompatible Changes

This Hardfork will activate 8 different CIPs (Conflux Improvement Proposals) including CIP-43, CIP-64, CIP-71, CIP-76, CIP-78, CIP-86, CIP-90, and CIP-92. For more details, see Upgrade CIPs: https://developer.confluxnetwork.org/v2-hardfork/upgrade_list/ 6

We suggest you pay more attention to CIP-43 and CIP-90:

- CIP-43: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-43.md 12 (Introducing a stand-alone PoS chain, which monitors the process of the PoW chain). For more details, see Conflux PoS Technical Documents: Conflux PoS Technical Documents
- CIP-90: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-90.md 2 (Introducing a new fully EVM-compatible space. The new space is called Conflux eSpace, and the current space is called Conflux Core). For more details, see Conflux eSpace Kit: Conflux eSpace Kit

Other Incompatible Changes:

- CIP-64: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-64.md 4
- CIP-71: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-71.md 1
- CIP-76: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-76.md 3
- CIP-78: https://github.com/Conflux-Chain/CIPs/blob/master/CIPs/cip-78.md 3

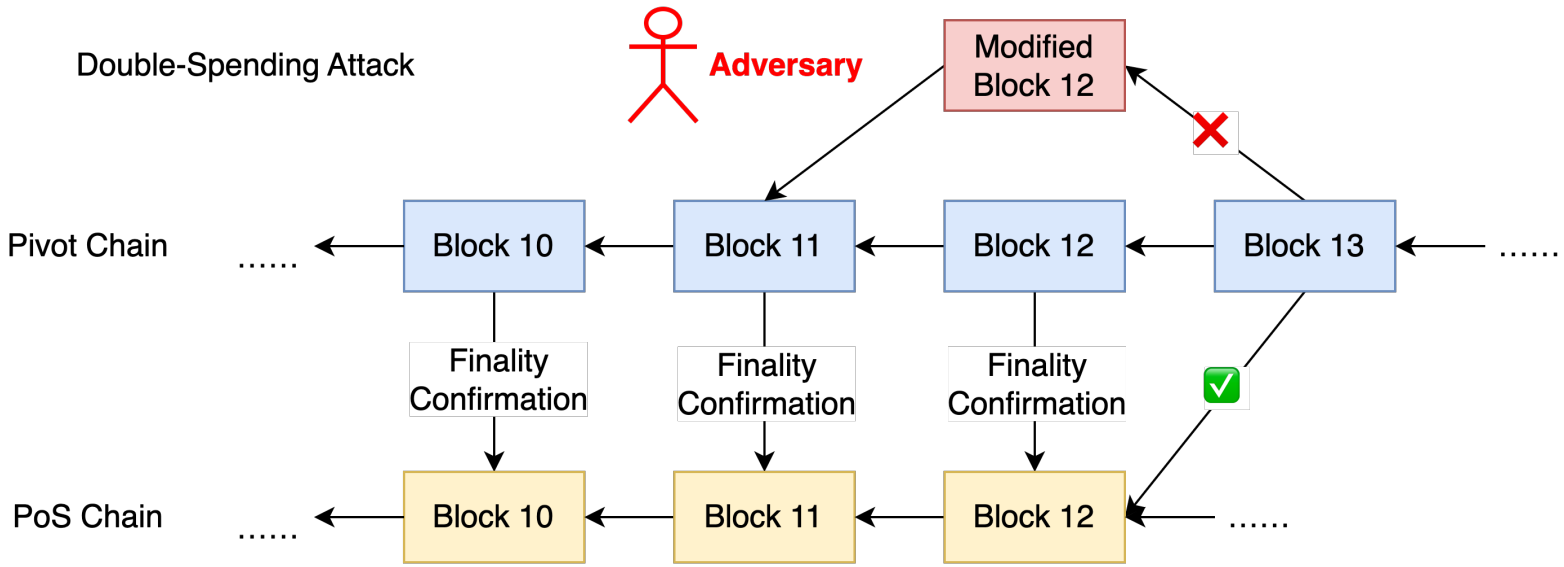
* CIP: Conflux Improvement Proposal, similar to EIP.

CIP-43: Introduce PoS Finality

- **Motivation:** reduce the risk of 51% attack from Ethereum miners.
- **Solution:**
  - Introduce a stand-alone PoS chain to confirm blocks from PoW Pivot Chain.
  - Establish a 300-member committee elected and rotated via VRF from stakers.
- **Security:** increase security threshold from 51% to 67%.
- **Result:** two parallel and independent chain
  - PoW for Tree-Graph consensus, PoS for finality confirmation.

CIP-43: Introduce PoS Finality

- **An example of potential double-spending attack**
  - Subsequent miners will follow the blocks confirmed by PoS chain.

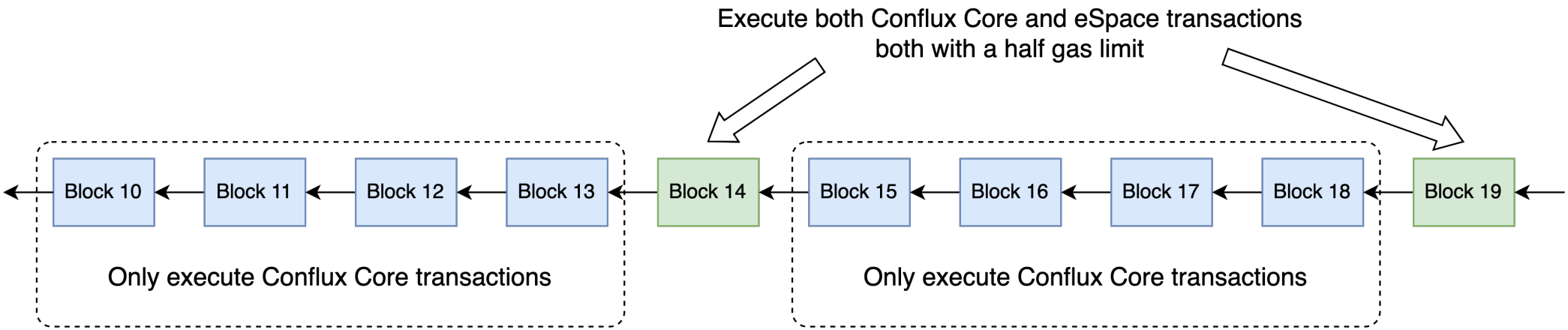


CIP-90: Introduce EVM Compatibility

- **Motivation: For the convenience of developers and dApp migration.**
  - Ethereum is currently the largest smart contract platform.
  - Different transaction format, address generation, Collateral for Storage, etc.
- **Solution: Divide one chain into two spaces, Core and eSpace.**
- **Result:**
  - fully compatible at the interface level, including RPC and EVM.
  - Basic tools of Ethereum can be directly used, e.g., Metamask, truffle, hardhat, Remix, ethers.js, web3.js.

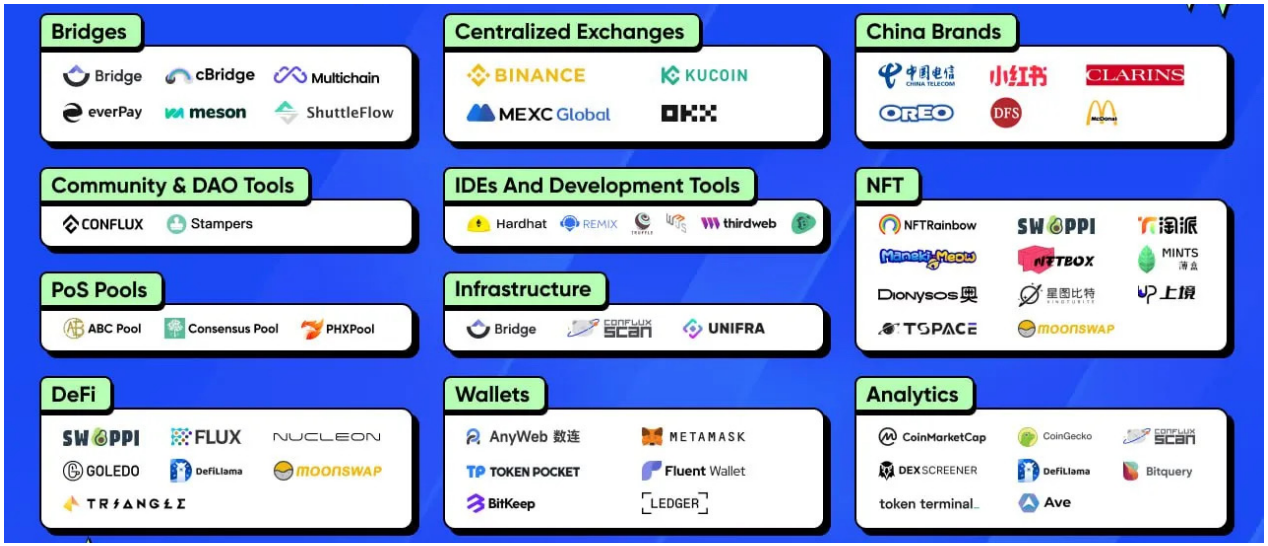
CIP-90: Introduce EVM Compatibility

- **Execute eSpace transactions every 5 blocks, with half of total gas limit of blocks.**



CIP-90: Introduce EVM Compatibility

- **Ecosystem: see prosperity since the hard fork.**
  - DeFi: DEX-Swappi, Lending-Goledo, Stablecoin-TriAngleDAO, Bridge-Multichain, etc.
  - Cooperation with China Telecom for blockchain-based SIM card in Hong Kong.



Part 3: Test Operations on the Testnet

- **Setting up**
  - Interact with blockchain: JSON-RPC
  - JavaScript runtime environment: node&npm
  - Construct and send transactions: js-conflux-sdk
  - Edit and deploy contract codes: ChainIDE
  - Manage our blockchain accounts and connect with external site: Plugin Wallets

Part 3: Retrieving blockchain data

Get blockchain status

```
{
  data: {
    jsonrpc: '2.0',
    id: '18770a0a2e6387a1ce44bfd7',
    method: 'cfx_getStatus',
    params: []
  },
  result: {
    bestHash: '0x487bf2ecae853b5c1ad5588b199049eef06f77374e7b5678482a44ddb130085
1',
    chainId: '0x1',
    ethereumSpaceChainId: '0x47',
    networkId: '0x1',
    epochNumber: '0x7110c78',
    blockNumber: '0x91697f7',
    pendingTxNumber: '0x224',
    latestCheckpoint: '0x70f8e60',
    latestConfirmed: '0x7110c31',
    latestState: '0x7110c74',
    latestFinalized: '0x7110a74'
  },
  duration: 861
}
```

Get balance of account

```
{
  data: {
    jsonrpc: '2.0',
    id: '187709e0d974f03c30cb678',
    method: 'cfx_getBalance',
    params: [ 'cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0' ]
  },
  result: '0xd51a279df7b0b3889800',
  duration: 1594
}
Balance: 1006346530907228000000000
```

Get next nonce

```
$ node main.js
{
  data: {
    jsonrpc: '2.0',
    id: '187709ce521b696b8c6c524b',
    method: 'cfx_getNextNonce',
    params: [ 'cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0' ]
  },
  result: '0xc92',
  duration: 1546
}
nonce: 3218
```

Part 3: Sending a transaction

Some information returned by the transaction

- next nonce
- epoch number
- gasPrice
- txHash


```
{
  data: {
    jsonrpc: '2.0',
    id: '18769247d9926bc53ab61525',
    method: 'txpool_nextNonce',
    params: [ 'cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0' ]
  },
  result: '0xc70',
  duration: 272
}
{
  data: {
    jsonrpc: '2.0',
    id: '18769247ebc8f36184cd02f8',
    method: 'cfx_epochNumber',
    params: []
  },
  result: '0x70e2ef2',
  duration: 217
}
{
  data: {
    jsonrpc: '2.0',
    id: '18769247f9cf57122b9f67b7',
    method: 'cfx_gasPrice',
    params: []
  },
  result: '0x3b9aca00',
  duration: 226
}
{
  data: {
    jsonrpc: '2.0',
    id: '187692480c4e7fab33b7b69a',
    method: 'cfx_sendRawTransaction',
    params: [
      '0xf875f1820c70843b9aca00825208941166f0e4fc2bb1a43d3d4ea6502b74c759caf753880de0b6b3a
65f639844b332fb173ecea89c3540da3ffe2183ed58274f6ae74433033'
    ]
  },
  result: '0x3e4de9eb4ff73555ceae490f9856c378a1b4958741418556a74f06e17a68ed20',
  duration: 212
}
time for this transaction: 1033ms
txHash: 0x3e4de9eb4ff73555ceae490f9856c378a1b4958741418556a74f06e17a68ed20
```

Part 3: The returned value of transaction

- Find the detailed information according to the hash.


```
result: {
  hash: '0x720aa3a10050f3ba7bca072eb2c9c951ae95f9d1cb1a1405a72175adae992f3a'
  nonce: '0x10c4',
  blockHash: null,
  transactionIndex: null,
  from: 'cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0',
  to: 'cfxtest:aaj0r6he9uz5dkb7hzhmpybnsxdzxw11mpa1kz35sz',
  value: '0xde0b6b3a7640000',
  gasPrice: '0x3b9aca00',
  gas: '0x5208',
  contractCreated: null,
  data: '0x',
  storageLimit: '0x0',
  epochHeight: '0x711442c',
  chainId: '0x1',
  status: null,
  v: '0x0',
  r: '0xe1016e375f4a9704774f6eafb11a2e0c3fc858481ba5621984017bbfd308e127',
  s: '0x6e6ad1c760048445d1bdb1a1d192c13e74c63b4a3dd380d91a002d4b8a38a01f'
},
```

Part 3: Smart Contracts Testing

- **CRC20 tokens, CRC721 tokens**
  - Refers to cryptocurrencies and NFTs, for Conflux Core

Transaction Hash	0xaf723392b8d149596e88d3dfaf2affc520e2b817faf82b9e8136cc8fbd0cf3a1
Executed Epoch	118,570,130
Proposed Epoch	118,570,123
Block Hash	0x574ad1dda97717180f2c2c0b5158e729e8ef6f72937886ca6e4ed11887ae391b
Timestamp	1 min 31 secs ago (2023-04-12 00:23:03 +08:00)
Status	Success
Security	Great 94 Epoch Confirmations
From	cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0
To	Contract cfxtest:aca979pkc3rnjgsm27kvvsa8u7c7b9b0jpfmyt5hhb Created
Value	0 CFX
Gas Fee	0.000910656 CFX

Transaction Hash	0xe253ffc6832e84066dd72299b32d7009a3bdf4ba4a1add5e5fbbddfca599aef1
Executed Epoch	118,570,552
Proposed Epoch	118,570,541
Block Hash	0xfcd49db263cd150fdd511ad76405a98fa68930f01bf45f388cc626eb8c9fd635
Timestamp	59 secs ago (2023-04-12 00:27:38 +08:00)
Status	Success
Security	Great 23 Epoch Confirmations
From	cfxtest:aanycwkmgw1gedjk9dmrp6k3h7f5m2zmuyd5wtaan0
To	Contract cfxtest:acddke192z3wyrcwcahbgjkv6ybm507h5uhptm5jzt Created
Value	0 CFX
Gas Fee	0.005629361 CFX

Part 3: Smart Contracts Testing

- **ERC20 tokens, ERC1155 tokens**
  - Refers to cryptocurrencies and NFTs, for Conflux eSpace (EVM)

Transaction Hash	0xe02b4773a2388323d7c00097ae1ffe59fceea8417046813d2063dea5a6805689
Block Height	118,765,290
Block Hash	0xff132a0af9716259743b54a03851de23181a9a604e6ee54ac76226209e7a9eea
Timestamp	53 secs ago (2023-04-13 13:33:14 +08:00)
Status	Success
Security	Great 54 Blocks Confirmations
From	0x0741492a34ae620d09f8d4d671393f4bb562aa85
To	Contract 0xf71cd5c932e9a2c048a2578095bb9355688b58bd Created
Value	0 CFX
Gas Fee	0.05410336 CFX

Transaction Hash	0x1214c600a57ec906f3400160609e095f6ee947245fc456b46c2ce8fb7b4a43dc
Block Height	118,765,585
Block Hash	0x6a79f1e5668c2d378ecddc5039288805aef2367c1d50e6eba747fa6e9b89d5a6
Timestamp	23 secs ago (2023-04-13 13:36:42 +08:00)
Status	Success
Security	Poor 0 Blocks Confirmations
From	0x0741492a34ae620d09f8d4d671393f4bb562aa85
To	Contract 0xbf7c2950c19ea1641023198e3d23c1147daa14f8 Created
Value	0 CFX
Gas Fee	0.1285938 CFX

Part 3: Performance Testing

- **Conflux Core Performance (500 transactions)**

  Send transactions by JS script

  gasPrice = 1000G drip(10^12), it uses 247 blocks, the TPS is 4.01

- **Conflux eSpace Performance (100 transactions)**

  Use a contract to send transactions

  The contract address is "0x9624bd1e6547ce5d53d09d336f87fd19f67fb18d"

  the TPS is 0.2

Part 3: Performance Testing - Analysis

SDK

- JavaScript is single-threaded

Query limitations

- The limitations of RPC services to interact with Conflux

Testing condition

- The actual mining speed is 2 blocks per second, with full execution process

Contract codes and scripts

- They can be improved from the perspective of performance

Part 4: Run an independent chain and analyze

- **Step 1: Start a boot node.**
  - Initialize the network, and open for new nodes to connect.
- **Step 2: Connect the wallet.**
  - Connect Fluent Wallet, the Conflux official plugin wallet.
- **Step 3: Start mining.**
  - We use CPU for mining computations.
- **Step 4: Start new nodes.**
  - Connect to the boot node and join the network.

* A video in the end to show the process.

Part 4: Run an independent chain and analyze

- **Existing Problems: (confirmed with Conflux team)**
  - The nodes are set in the same LAN in order to ensure RPC connection, otherwise the forwarding of router NAT requires manual settings.
  - “min_phase_change_normal_peer_count” is “3” by default: otherwise the network will never enter the normal phase.
  - simply selecting or scrolling the output command line will make the thread stuck in Windows 10.

Part 4: Run an independent chain and analyze

- **Interesting Finding 1:**
  - Checkpoint Mechanism: Save local storage.

```
2023-04-08T21:04:40.253850800+08:00 INFO  main                conflux      - Conflux client started
2023-04-08T21:04:41.213958600+08:00 INFO  IO Worker #0        cfxcore::syn - start phase "CatchUpRecoverBlockHeaderFromDbPhase"
2023-04-08T21:04:41.216754600+08:00 WARN  IO Worker #3        network::ser - No peers connected at this moment, 0 pending + 0 started
2023-04-08T21:04:41.218551900+08:00 INFO  IO Worker #0        cfxcore::syn - Catch-up mode: true, latest epoch: 0 missing_bodies: 0
2023-04-08T21:04:41.220710700+08:00 INFO  unnamed             cfxcore::syn - Start fast recovery of the block DAG from database
2023-04-08T21:04:41.222574400+08:00 INFO  unnamed             cfxcore::syn - finish recover header graph from db
2023-04-08T21:04:42.223650100+08:00 WARN  IO Worker #3        network::ser - No peers connected at this moment, 0 pending + 0 started
2023-04-08T21:04:42.225005900+08:00 INFO  IO Worker #1        cfxcore::syn - start phase "CatchUpSyncBlockHeaderPhase"
2023-04-08T21:04:42.226078900+08:00 INFO  IO Worker #1        cfxcore::syn - start phase "CatchUpCheckpointPhase"
2023-04-08T21:04:42.228322100+08:00 INFO  IO Worker #1        cfxcore::syn - CatchUpCheckpointPhase: commitment for epoch
0x147ee7fe6c62da144ab38a29dbd006a20761c37d444e4396392a9938ddb34d28 exists, skip state sync. commitment=EpochExecutionCommitment
{ state_root_with_aux_info: StateRootWithAuxInfo { state_root: StateRoot { snapshot_root:
0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470, intermediate_delta_root:
0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470, delta_root:
0x93c92be2f0be359be111d90cdc9849d42c364ea311f5a8c9207bf8cfa0227d76 }, aux_info: StateRootAuxInfo { snapshot_epoch_id:
0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470, intermediate_epoch_id:
0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470, maybe_intermediate_mpt_key_padding: None, delta_mpt_key_padding:
DeltaMptKeyPadding([156, 107, 44, 27, 13, 11, 37, 160, 8, 230, 200, 130, 204, 123, 65, 95, 48, 153, 101, 199, 42, 210, 185, 68, 172, 9, 49,
4, 140, 163, 28, 213]), state_root_hash: 0x7dd1a9ef0ad395b8fafa9c8fc71dd88bf21617fc6eefcf970a716151f7728acd } }, receipts_root:
0x09f8709ea9f344a810811a373b30861568f5686e649d6177fd92ea2db7477508, logs_bloom_hash:
0xd397b3b043d87fcd6fad1291ff0bfd16401c274896d8c63a923727f077b8e0b5 }
```

Part 4: Run an independent chain and analyze

- **Interesting Finding 2:**
  - The return value when a node mines a new block
    - parent_hash and referee_hash

```
2023-04-08T21:05:38.090253100+08:00 INFO  mining               cfxcore::syn - Mined block
0x80ee22cc302846fc807c8b6bd2f97f6780ac1bf5b8e4f3c676cca207413f821b header=BlockHeader { rlp_part: BlockHeaderRlpPart { parent_hash:
0xaa48b623e6e00a189e5bbfbf0f72ff45bbfd81da3b35cd7e338f550fb8de02b0, height: 6, timestamp: 1680959138, author:
0x12c9c116fc8b410ce2f98b5ed2a911a2af254d5d, transactions_root: 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470,
deferred_state_root: 0x9df37a2966022d302f269464cdbac5442b8e0d154ba9433476b3eec511acb756, deferred_receipts_root:
0x09f8709ea9f344a810811a373b30861568f5686e649d6177fd92ea2db7477508, deferred_logs_bloom_hash:
0xd397b3b043d87fcd6fad1291ff0bfd16401c274896d8c63a923727f077b8e0b5, blame: 0, difficulty: 4, adaptive: false, gas_limit: 30000000,
referee_hashes: [], custom: [], nonce: 6827236959887047447, pos_reference: None }, hash:
Some(0x80ee22cc302846fc807c8b6bd2f97f6780ac1bf5b8e4f3c676cca207413f821b), pow_hash: None, approximated_rlp_size: 384 }
```

Part 4: Run an independent chain and analyze

- **Interesting Finding 3:**
  - Special configurations related to the new features.

```
# The chain ID of Conflux Network (Conflux space)
# 1 for testnet
# 1029 for Mainnet (Hydra)
#
chain_id = 6290

# The EVM chain ID of Conflux Network (EVM space)
# 1030 for Mainnet (Hydra)
#
evm_chain_id = 6291
hydra_transition_number = 92060600
hydra_transition_height = 36935000
cip43_init_end_number = 92751800
pos_reference_enable_height = 37400000
```