Scroll Pre-Alpha Testnet Upgrade

Ye Zhang
Cofounder @ Scroll
What is Scroll?

A scaling solution for Ethereum
What is Scroll?

An **EVM-equivalent** zk-Rollup
Outline

• The architecture of Scroll
• The workflow of Scroll
• Scroll Pre-Alpha Testnet Upgrade
• The roadmap
The architecture of Scroll
zkRollup

Smart Contract

data

proof

Layer 2 node

TX_1

TX_2

......

TX_n
Scroll Architecture

- Bridge Contract
- Rollup Contract
- Sequencer
- Relayer
- Proof
- Data

Transactions: $TX_1$, $TX_2$, $TX_n$
Scroll Architecture

- Bridge Contract
- Rollup Contract

- Sequencer
- Coordinator
- Roller
- zkEVM

- Decentralized Prover Network

Data flow:
- \( TX_1 \)
- \( TX_2 \)
- \( TX_n \)
Scroll Architecture – what happens in the Roller?

Received from Coordinator

Execution Trace
Scroll Architecture – what happens in the Roller?

- Received from Coordinator
- Witness
  - zkEVM
  - EVM Circuit
  - RAM Circuit
  - Storage Circuit
  - Other Circuits

Execution Trace ➔ Circuit Input Builder
Scroll Architecture – what happens in the Roller?

- **Execution Trace**
- **Circuit Input Builder**
- **zkEVM**
  - **EVM Circuit**
  - **RAM Circuit**
  - **Storage Circuit**
  - **Other Circuits**
- **Aggregation Circuit**
- **Block Proof**

**Received from Coordinator**

**Witness**

**Proof**
The workflow of Scroll
The workflow of zk-Rollup

block data
validity proof
The workflow of Scroll’s zk-Rollup

- Block data
- Validity proof
L2 Block status

• **Pre-committed**: indicates a block has been proposed by a Sequencer and included in the L2 chain.

• **Committed**: indicates the transaction data of this block has been posted on the rollup contract on Ethereum.

• **Finalized**: indicates the correct execution of transactions in this block has been proven by verifying a validity proof on-chain on Ethereum.
The workflow of Scroll’s zk-Rollup

- Rollup Contract
- Sequencer
- Coordinator
- Roller 1
- Roller 2
- Roller 3
- Roller 4

Time

- Data
- Trace
- Proof
- Pre-committed Block
- Committed Block
- Finalized Block
The workflow of Scroll’s zk-Rollup

1. Rollup Contract
2. Sequencer
3. Coordinator
4. Roller 1
5. Roller 2
6. Roller 3
7. Roller 4

- Data
- Trace
- Proof
- Pre-committed Block
- Committed Block
- Finalized Block

Time
The workflow of Scroll’s zk-Rollup

Rollup Contract

Sequencer

Coordinator

Roller 1

Roller 2

Roller 3

Roller 4

Data
Trace
Proof
Pre-committed Block
Committed Block
Finalized Block

Time
The workflow of Scroll’s zk-Rollup

- **Rollup Contract**
  - D1

- **Sequencer**
  - 1

- **Coordinator**
  - T1

- **Roller 1**
  - Proof generation

- **Roller 2**

- **Roller 3**

- **Roller 4**

**Time**

- **Proof**
- **Data**
- **Trace**
- **Pre-committed Block**
- **Committed Block**
- **Finalized Block**
The workflow of Scroll’s zk-Rollup

1. Data (D1) is received by the Rollup Contract.
2. Trace generation (T1) occurs in the Sequencer.
3. Data is passed to the Coordinator (T1).
4. Coordinator generates Proof (T2).
5. Proof generation (D2) is sent to the Rollers.
6. Proof is verified and committed in the Rollers.
7. Finalized block is generated and sent to the Coordinator.

Time progression from left to right.
The workflow of Scroll’s zk-Rollup

- **Rollup Contract**
  - D1
  - D2
  - D3
  - D4

- **Sequencer**
  - 1
  - 2
  - 3
  - 4

- **Coordinator**
  - T1
  - T2
  - T3

- **Roller 1**
  - Proof generation

- **Roller 2**
  - Proof generation

- **Roller 3**
  - Proof generation

- **Roller 4**

Legend:
- Data
- Trace
- Proof
- Pre-committed Block
- Committed Block
- Finalized Block

Time
The workflow of Scroll’s zk-Rollup

- **Rollup Contract**
  - D1
  - D2
  - D3
  - D4

- **Sequencer**
  - 1
  - 2
  - 3
  - 4

- **Coordinator**
  - T1
  - T2
  - T3
  - P1
  - P2
  - P3

- **Roller 1**
  - Proof generation

- **Roller 2**
  - Proof generation

- **Roller 3**
  - Proof generation

- **Roller 4**

**Time**

- Data
- Trace
- Proof
- Pre-committed Block
- Committed Block
- Finalized Block
The workflow of Scroll’s zk-Rollup

1. **Proof generation**
2. **Proof generation**
3. **Proof generation**
4. **Aggregate proof generation**

**Data**

**Trace**

**Proof**

**Pre-committed Block**

**Committed Block**

**Finalized Block**

**Time**
The workflow of Scroll’s zk-Rollup

Rollup Contract

Sequencer

Coordinator

Roller 1

Roller 2

Roller 3

Roller 4

Proof generation

Proof generation

Proof generation

Aggregate proof generation

Data
Trace
Proof
Pre-committed Block
Committed Block
Finalized Block

Time
The workflow of Scroll’s zk-Rollup

- **Rollup Contract**: D1, D2, D3, D4
- **Sequencer**: 1, 2, 3, 4
- **Coordinator**: T1, T2, T3
- **Roller 1**: Proof generation
- **Roller 2**: Proof generation
- **Roller 3**: Proof generation
- **Roller 4**: Aggregate proof generation
- **Verify**: A

**Time**
The workflow of Scroll’s zk-Rollup

1. **Proof generation**
   - D1
   - D2
   - D3
   - D4

2. **Coordinator**
   - T1
   - T2
   - T3
   - P1
   - P2
   - P3

3. **Roller 1**
   - Proof generation

4. **Roller 2**
   - Proof generation

5. **Roller 3**
   - Proof generation

6. **Roller 4**
   - Aggregate proof generation

7. **Verify**
Rollup explorer shows the block status

<table>
<thead>
<tr>
<th>L2 Block No.</th>
<th>Block Hash</th>
<th>Tx(s)</th>
<th>Timestamp</th>
<th>Status</th>
<th>Commit Tx Hash</th>
<th>Finalize Tx Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>31538</td>
<td>0xcea1...773</td>
<td>1</td>
<td>a few seconds ago</td>
<td>Precomitted</td>
<td>0x5310...b6b1</td>
<td>-</td>
</tr>
<tr>
<td>31537</td>
<td>0xe46c...1109</td>
<td>1</td>
<td>a minute ago</td>
<td>Committed</td>
<td>0xfeb8...4dc3</td>
<td>-</td>
</tr>
<tr>
<td>31536</td>
<td>0x1143...d5da</td>
<td>1</td>
<td>a minute ago</td>
<td>Committed</td>
<td>0xe491...7baa</td>
<td>-</td>
</tr>
<tr>
<td>31535</td>
<td>0x620d...87c7</td>
<td>1</td>
<td>2 minutes ago</td>
<td>Committed</td>
<td>0xc544...7c07</td>
<td>-</td>
</tr>
<tr>
<td>31534</td>
<td>0x0f46...b3d4</td>
<td>1</td>
<td>2 minutes ago</td>
<td>Committed</td>
<td>0x9fa9...f81f</td>
<td>-</td>
</tr>
<tr>
<td>31533</td>
<td>0xd12b...cc54</td>
<td>1</td>
<td>2 minutes ago</td>
<td>Committed</td>
<td>0x3625...0054</td>
<td>-</td>
</tr>
</tbody>
</table>
Rollup explorer shows the block status

<table>
<thead>
<tr>
<th>Last Pre-committed Block No.</th>
<th>Last Committed Block No.</th>
<th>Last Finalized Block No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>31540</td>
<td>31540</td>
<td>31444</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L2 Block No.</th>
<th>Block Hash</th>
<th>Tx(s)</th>
<th>Timestamp</th>
<th>Status</th>
<th>Commit Tx Hash</th>
<th>Finalize Tx Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>31440</td>
<td>0x3803...7a7e</td>
<td>1</td>
<td>18 minutes ago</td>
<td>Committed</td>
<td>0xb9cc...7c20</td>
<td>-</td>
</tr>
<tr>
<td>31439</td>
<td>0x37f9...b121</td>
<td>2</td>
<td>18 minutes ago</td>
<td>Committed</td>
<td>0x1d61...712e</td>
<td>-</td>
</tr>
<tr>
<td>31438</td>
<td>0xd4c6...0ed6</td>
<td>4</td>
<td>18 minutes ago</td>
<td>Finalized</td>
<td>0x1d61...712e</td>
<td>0xfb88...4dc3</td>
</tr>
<tr>
<td>31437</td>
<td>0xcd6e...dd14</td>
<td>3</td>
<td>18 minutes ago</td>
<td>Finalized</td>
<td>0x1d61...712e</td>
<td>0x4e91...7baa</td>
</tr>
<tr>
<td>31436</td>
<td>0x7c87...8ac5</td>
<td>2</td>
<td>18 minutes ago</td>
<td>Finalized</td>
<td>0x1d61...712e</td>
<td>0x4e91...7baa</td>
</tr>
<tr>
<td>31435</td>
<td>0x798e...0f85</td>
<td>2</td>
<td>19 minutes ago</td>
<td>Finalized</td>
<td>0x432c...dfaa</td>
<td>0xc544...7c07</td>
</tr>
</tbody>
</table>
Scroll Pre-Alpha Testnet
Three months ago, we have released our testnet

- Users can play with pre-deployed DApps through metamask
- Users can bridge their asset between L1 and L2
- Users can see their Tx status through Rollup explorer
Three months ago, we have released our testnet

- We'd like to thank the community for their helpful feedback!
- We have onboarded over 10k users to test bridge and DApps
- Scale up our proving infrastructure to support 100K+ users on waitlist!
Announcement: The upgrade!
The upgrade of our Pre-Alpha Testnet

• Support arbitrary smart contract deployment!
  ○ Seamless migration without any need to change the code!
  ○ Support all the toolings around (Remix, Harhat, Foundry, etc)!

• Hackathon at ETH Global and Open register to all developers
Pre-Alpha Testnet

To become an early tester and contributor
Sign up at https://scroll.io/early-dev
A summary for users and developers

• The developer experience will be exactly the same as Ethereum

• Layer 2 block generation takes <3 seconds

• Deposit takes 2 minutes (wait for 6 L1 blocks to be safe)

• Withdraw takes more than 6 minutes (depends on prover & TPS)
Our roadmap
Roadmap

PHASE 1
Pre-Alpha testnet

PHASE 2
Alpha testnet

PHASE 3
Layer-2 proof outsourcing

PHASE 4
zkEVM mainnet

PHASE 5
Decentralized sequencer
more efficient zkVM
Our plan for hardware acceleration

Stage 1
zkEVM GPU cluster

- We have built a very fast GPU solution to generate proofs for zkEVM circuits (1M gas takes 6 minutes)
- We have built a private GPU cluster to provide more stable computation power for our Testnet in Stage 1
- We are collaborating with companies on more customized hardware acceleration (FPGA, ASIC and GPU)
Our plan for hardware acceleration

Stage 1
zkEVM GPU cluster

Stage 2
Integrate with hardware partners
(FPGA/GPU/ASIC provers)

- We will give access to hardware partners and they can test their prover and generate proofs for us
- Customized provers can significantly shorten the finality time and improve UX
Our plan for hardware acceleration

Stage 1
zkEVM GPU cluster

Stage 2
Integrate with hardware partners
(FPGA/GPU/ASIC provers)

Stage 3
Permissionless prover
(anyone can run a prover node)

- We will open-source our GPU prover with a permissionless license for everyone to use
- The prover access will become permissionless, anyone can be Roller and generate proof for us
- They can also buy customized hardware from hardware companies/stake to use some prover service
One Last thing!
Our tech team

• Infrastructure team (Asia & Europe)

• zk team (Asia & US)

• Security team

• Research team
Our vision

• Onboard the next billion of users for Ethereum

• Build in the open, co-build with community

• Fight for decentralization across different levels
We are hiring! Check out [jobs.lever.co/ScrollFoundation](http://jobs.lever.co/ScrollFoundation)
Thank you!

@yezhang1998