Roll-ups

1. Introduction

Blockchains are incredibly secure, but that comes at a price. While most blockchains are safe by design, that can greatly impact their speed and transaction prices. While every system can cope with thousands of transactions at a time many blockchain networks are limited in that respect. In particular, networks like Ethereum carry high gas fees and slow transaction times that have been persistent issues for users. Furthermore, as you improve a blockchain's scalability, it also impacts its security and decentralisation. This is known as the blockchain trilemma, and there are a few different methods of combating its effects. However, blockchain roll-ups help in executing transactions efficiently.

- **Definition of Roll-ups**
    - Blockchain rollups refer to a layer 2 crypto scaling solution for blockchains which involves 'rolling up' or compiling a bunch of transactions on a layer 2 blockchain and turning them into a single piece of data to broadcast on a Layer 1 blockchain. To explain, they take the transactions out of the main net and process them off-chain. Then convert them into one single piece of data, and submit them back on a parent chain. This is why rollups are also called 'off-chain scaling solutions.'
    - The regular blocks on most blockchain networks can only store a limited amount of data. Since there is limited space in each block, the network takes more time to process transactions. While the main net prioritises a selected transaction with the highest bids, all other transactions would have to wait. The more users and applications on the main blockchain, the more the network traffic increases. This can make transactions extremely slow and costly, no matter their contents. In such cases, roll-ups take transactions out of the main net, convert them into a single piece of data and add them back. This makes transactions faster, and more efficient and allows more data to be stored.
- **Purpose of the Research**

  To understand the various techniques and methodologies to scale and make the blockchain network much more efficient.
  Understanding the mathematical significance of Layering 2 solutions such as Rollups.
  To build an understanding of the Rollups mechanism to further enhance these techniques or come up with better alternatives which might increase the efficiency.

2. Historical Background

- **Origin of Roll-ups**
    - **Scalability Challenges:** The need for roll-ups arose due to the scalability limitations of early blockchain networks, particularly Ethereum. As

blockchain adoption grew, networks like Ethereum struggled with congestion in transactions, leading to high transaction fees which are commonly called gas fees and slow processing times.

- **Introduction of Roll-Ups:** The concept of roll-ups was introduced as a Layer 2 scaling solution to address these challenges. Vitalik Buterin, Ethereum's co-founder, and other developers began exploring roll-ups as a way to improve Ethereum's scalability without sacrificing security or decentralisation.

- **Evolution Over Time**
  - **2014-2015: Early Research and Concepts**

    The idea of off-chain computation and data compression to improve blockchain scalability was discussed in the early days of Ethereum. However, the specific concept of roll-ups had not yet emerged.

  - **2018: Plasma**

    Plasma, proposed by Vitalik Buterin and Joseph Poon, was one of the early Layer 2 solutions that laid the groundwork for roll-ups. Plasma chains work by creating "child chains" that could process transactions off-chain while periodically committing the results to the Ethereum main-net. Although Plasma wasn't a roll-up, it shared some conceptual similarities.

  - **2019: Introduction of ZK-Rollups and Optimistic Rollups**

    ZK-Rollups (Zero-Knowledge Rollups): Eli Ben-Sasson and others at StarkWare developed ZK-Rollups, which use zero-knowledge proofs to bundle multiple transactions into a single proof that is submitted to the Ethereum main-net. This method ensures security and reduces the amount of data required on-chain.

    Optimistic Rollups: Another type of roll-up, optimistic rollups, emerged as a simpler alternative. Optimistic rollups assume that transactions are valid by default and only run computations in the case of a challenge. This reduces the computational burden on the main chain.

  - **2020: Ethereum 2.0 and Roll-Ups as the Future of Scaling**

    Vitalik Buterin emphasised roll-ups as a crucial part of Ethereum's scaling roadmap. Ethereum 2.0's transition to proof-of-stake (PoS) was designed to work hand-in-hand with roll-ups, which were expected to handle most of the transaction processing.

  - **2021: Deployment of Roll-Ups on Ethereum**

Several projects launched roll-up solutions on Ethereum, including:

Optimism: A leading implementation of optimistic rollups.

Arbitrum: Another prominent optimistic rollup solution.

zkSync and Loopring: Both employ ZK-rollups, offering significant reductions in transaction costs while maintaining security.

- **2022-2023: Roll-Ups Gain Adoption**

  Roll-ups became a key component of Ethereum's scalability strategy. Major DeFi projects began integrating with roll-up solutions to reduce fees and improve user experience.

  zkEVMs: The development of zkEVMs (zero-knowledge Ethereum Virtual Machines) advanced ZK-rollups by making them fully compatible with existing Ethereum smart contracts.

- **2023 Onwards:**

  The continued improvement and adoption of roll-ups are expected to be integral to the future of blockchain scaling, particularly for Ethereum, as they aim to handle a significant portion of the network's transaction load.

3. Types of Roll-ups

- **Overview of Different Roll-up Models**
  - There are two main types of rollups, Optimistic and Zero-Knowledge (ZK). The benefit of either is they cut down transaction costs (like Ethereum gas fees) considerably. The idea is that instead of waiting and paying for each transaction to process independently on Ethereum, dozens and dozens of transactions are recorded on the layer 2 chain, then "rolled up" into a single transaction that is then fed back to the more expensive, slower blockchain. By doing this, the cost of that one transaction is split across lots of users.
- **Zero-Knowledge (ZK) Roll-ups**
  - The first kind of rollup is a Zero-Knowledge rollup, also known as a ZK-rollup. These protocols use a complex piece of cryptography called a Zero-Knowledge proof to determine that a transaction is valid using only minimal information about that transaction. It's privacy-preserving, sleek and, most important, fast and cheap. Compared with an Optimistic rollup, which requires funds to stay on the network until the dispute resolution period has closed, ZK-rollups allow users to withdraw their funds with less of a delay.

- **Optimistic Roll-ups**
    - Optimistic Rollups assume that transactions are valid by default and only execute a transaction on layer 1 if someone challenges its validity. If a transaction is found to be invalid, a fraud-proof mechanism is triggered, and the incorrect transaction is rolled back. Optimistic Rollups are compatible with the Ethereum Virtual Machine (EVM), making it easier to port existing dApps to this layer 2 solution.
    - By assuming that most transactions are valid, Optimistic Roll ups reduce the need to store and process data on the layer 1 chain, leading to lower fees and higher scalability. One of the most popular Optimistic Rollup solutions, Arbitrum, aims to provide faster and cheaper transactions while maintaining a high level of security.

4. Technical Architecture

- **Core Components**
    - **Rollup Operator**

      It is the main component that powers and manages all the activity of the Rollup. It looks after the collection of data and the orders along with it, it then processes the transaction off-chain (Layer 2). The basic steps include:

      1) **Transaction collection**: It gathers all the transaction data and information off-chain for it to be further examined and processed.
      2) **Batching**: It groups these data into a single batch in order to reduce the load on the main chain by compressing the data.
      3) **Proof Generation**: Based on the type of Rollup being used (eg- ZK rollup), it may generate a proof known as validity proof in order to show that the transaction is valid and can be added to the main chain now.
    - **Smart Contracts**

      These are deployed in the main chain and handle the logic for verifying and finalising the transactions, they use proofs and other mechanisms to do so. They are important as they provide Rollup input and output verification. Its functions include:

      1) **Managing Deposits and Withdrawals**: These securely handle the movement of transactions between layer 1 and layer 2, hence handling the input and output of the funds and transactions.

      2) **Verification**: These check the validity of the batches that the Rollup provides after the successful processing of the transaction through logic and proof to prevent fraudulent activity.

3) **State Management**: These maintain the state of the Rollup on the main chain, ensuring that the information on layer 1 reflects on layer 2 and that the security traits of layer 1 are present in layer 2 as well.

- **Merkle Tree**

  It is a cryptographic structure or a data structure that efficiently organises and verifies data. For Rollups:

  1) **Data Integrity**: It makes sure that any minor change in the data would result in changes in the entire tree, hence, making it easy to detect any tampering and keep the data safe.
  2) **Efficient Verification**: Only a significant amount of data needs to be stored in Layer 1, it's called a Merkle Root, it represents all the transactions in the Rollups. Anyone can look into the Merkle root to verify the validity of a transaction.

- **How Rollups Work**

  The step-by-step process is as follows:

  1) **Collecting Transactions:** Transactions are collected on layer 2, which is an off-chain environment where the processing takes place and transactions are handled at lower costs. Users interact similarly with layer 2 but everything happens quickly and cheaply.
  2) **Batching Transactions:** In this process, all the transactions are compressed into a single batch, this helps in reducing the space and faster execution. The batch includes all the necessary information regarding the transactions.
  3) **Submitting to layer 1:** The batch is then sent to the main chain along with a validity proof (In case of ZK rollups) or just the batch (In case of optimistic rollups). The submission tells the blockchain that this is the data that was processed off-chain.
  4) **Verification at Layer 1:** The smart contracts on Layer 1 verify the batch. In zk-Rollups, this involves checking the cryptographic proof to ensure that the transactions are valid. In Optimistic Rollups, the transactions are assumed valid unless someone challenges them with fraud-proof. Once verified, the transactions are finalised, meaning they are permanently recorded on the main blockchain.

- **Security Mechanisms**
  - **Data Availability:** Ensuring data availability is crucial for the security of roll-ups. If transaction data is unavailable or lost, users could lose access to their funds or be unable to validate the correctness of transactions.
    - **On-Chain Data:** In some roll-up designs, the transaction data or its summary is posted on the main chain, ensuring that all necessary information is always available.

        - **Off-Chain Data Availability Committees:** Some roll-ups use data availability committees to hold and distribute the data, but this requires trust in the committee members. This approach is more common in hybrid models.
        - **Data Availability Proofs:** Advanced roll-ups are exploring the use of data availability proofs to ensure that off-chain data is always accessible and verifiable.
    - **Withdrawal Periods:** Roll-ups often implement a withdrawal period to allow time for challenges or proofs to be submitted before funds can be withdrawn to the main chain.
        - **Delayed Finality:** After initiating a withdrawal from a roll-up to the main chain, users must wait for the withdrawal period to end. This delay allows time for potential fraud proofs or disputes to be resolved.
        - **Security Assurance:** This period ensures that if any invalid transactions were included in a roll-up batch, they can be caught and rectified before funds are moved.
    - **Crypto-economic Consensus:** Roll-ups often rely on a form of crypto-economic consensus among participants to ensure that the transactions processed off-chain are valid and that the roll-up is behaving correctly.
        - **Consensus among Validators:** Some roll-ups might use a committee of validators to agree on the state before it's posted to the main chain, adding an additional layer of security.
        - **Staking:** Participants might stake tokens to become validators or operators, which can be slashed if they act dishonestly, thereby securing the network through economic incentives.
    - **Regular State Commitment:** Roll-ups periodically commit the state of the off-chain transactions to the main chain to ensure that the blockchain's security is extended to the roll-up.
        - **State Roots:** The roll-up regularly posts the root of the Merkle tree (which represents the state of all accounts and balances) to the main chain. This allows anyone to verify the state of the roll-up on-chain.
        - **Consistency Checks:** This ensures that the state of the roll-up is consistent and that any tampering or errors in the off-chain data would be detectable when compared with the on-chain state.
    - **Economic Incentives:** Economic incentives are used to align the behaviour of participants with the security goals of the roll-up.
        - **Bonding and Slashing:** Operators of the roll-up may be required to post a bond that can be slashed if they act maliciously. This provides a financial disincentive for dishonest behaviour.
        - **Rewards for Validators/Challengers:** Validators or users who submit valid fraud proofs are often rewarded. This incentivizes vigilant monitoring of the roll-up's transactions.

- **Specific to Optimistic Roll Ups**

  Fraud Proofs: In optimistic roll-ups, transactions are assumed to be valid by default. However, to prevent malicious activity, fraud proofs are used. If someone suspects that a batch of transactions is invalid, they can submit a fraud-proof to the main chain.

  - **Challenge Period:** After a roll-up submits a batch, there's a challenging period during which anyone can dispute the validity of the transactions by submitting a fraud-proof.
  - **Dispute Resolution:** If a fraud-proof is submitted, the roll-up must provide evidence to validate the disputed transaction. If the roll-up is unable to prove the validity, the transaction batch is considered fraudulent, and the state is reverted.
  - **Incentives:** To discourage bad actors, the party that successfully challenges an invalid transaction typically receives a reward, while the roll-up operator may lose their stake.
- **Specific to ZK Roll Ups**

  Validity Proofs: ZK-Rollups use zero-knowledge proofs (specifically, succinct non-interactive arguments of knowledge, or zk-SNARKs) to ensure the validity of transactions without revealing any transaction details.

  - **Zero-Knowledge Proofs:** For each batch of transactions, a cryptographic proof is generated that attests to the correctness of all transactions within the batch. This proof is then submitted to the main chain.
  - **On-Chain Verification:** The main chain verifies the zero-knowledge proof. If the proof is valid, it guarantees that all transactions in the batch are valid. This eliminates the need for a challenge period, as the proof itself is a strong guarantee of validity.
  - **Trustless Security:** Because zk-SNARKs are mathematically sound, the security of ZK-Rollups relies on cryptographic principles, making it extremely difficult for a bad actor to create a fraudulent proof.

- **Performance Metrics**

Sl. No.	Name of KPI	Description	Importance	Target Metric
1.	Total Value Locked (TVL)	The total amount of assets (in USD or crypto terms) locked within the roll-up's smart contracts.	TVL is a strong indicator of user trust and the roll-up's adoption. Higher TVL suggests that users are confident in the security and reliability of the roll-up.	Increasing TVL over time, indicating growing adoption and trust.

2.	Transaction Throughput	Measures the number of transactions a roll-up can process per second (TPS).	High transaction throughput is a key advantage of roll-ups, as they aim to scale blockchain networks by processing more transactions off-chain while still benefiting from Layer 1 security.	A high TPS, typically much greater than what the underlying Layer 1 blockchain can handle, indicates efficient scaling.
3.	Transaction Latency	The time it takes for a transaction to be processed and finalised on the roll-up.	Lower latency means faster transaction confirmations, which is crucial for user experience, especially in applications like DeFi and gaming.	Low latency, ideally comparable to or better than Layer 1 solutions.
4.	Gas Fees	The average cost for users to execute transactions on the roll-up.	One of the primary goals of roll-ups is to reduce transaction costs. Lower fees make the roll-up more attractive to users and drive higher adoption.	Significantly lower transaction costs compared to the underlying Layer 1 blockchain, often by an order of magnitude.
5.	Finality Time	The time it takes for transactions on the roll-up to be considered final and irreversible on the underlying Layer 1 blockchain.	Shorter finality times improve the user experience and reduce the risk of reorganisation attacks.	Fast finality times that are competitive with or better than those of Layer 1, depending on the specific roll-up design (e.g., Optimistic Roll-ups vs. ZK-Rollups).
6.	Roll Up Operator Decentralisation	Measures the decentralisation of the entities or nodes that operate the roll up.	A decentralised operator structure is critical for reducing the risk of centralisation-related issues, such as censorship or collusion,	A large number of independent operators or validators, contribute to the network.
7.	Fraud/Validity proof verification Time	The time it takes for the main chain to verify fraud or validity proofs submitted by the roll ups.	Faster verification times enhance security and security and reduce the window for potential attacks or fraud.	Minimum time required for proof verification while maintaining high-security standards.
8.	Rollback or Reorg Resistance	The roll up's ability to resist rollbacks or reorgs on the	Ensuring that roll ups are resistant to Layer 1 reorgs protects users from potential loss of funds or state	Strong resistance to reorgs with mechanisms to

		underlying Layer 1 chain.	inconsistencies.	mitigate their impact.

5. Applications and Use Cases

- **In Finance**

  Rollups have significant potential in financial systems and transactions due to their ability to enhance scalability, reduce costs, and maintain security. Some of its uses are:

  1. **High-Frequency Trading(HFTs):** Rollups can bundle many trades and transactions into a single one, reducing latency and costs, hence making HFTs more efficient.
  2. **Payment Processing:** Rollups aggregate payments, lowering fees and speeding the settlements, especially useful for micropayments and remittances.
  3. **Decentralised Exchanges(DEXs):** Roll Ups help reduce On-chain transactions, lowering fees and increasing the speed of trades on DEXs.
  4. **Lending and borrowing:** Rollups process loans off-chain, reducing costs and making DeFi lending faster and more accessible.
  5. **Clearing and Settlement:** Rollups speed up the settlement process, reducing the time and risk compared to traditional financial systems.

- **In Blockchain**
  - In the blockchain space, roll-ups are a Layer 2 scaling solution that aggregates transactions or operations off-chain and then submits a single batch to the main blockchain (Layer 1). This approach reduces the load on the main blockchain, leading to faster transactions and lower fees. Here are some examples of roll-ups in blockchain.
- **In Other Industries**
  1) **Supply Chain Management:** Rollups can aggregate and verify supply chain transactions off-chain, ensuring transparency and traceability while reducing costs associated with blockchain transactions.
  2) **Healthcare:** Rollups can securely manage and process large volumes of patient records and medical transactions off-chain, ensuring privacy and reducing the load on the main blockchain.
  3) **Gaming:** Rollups can handle in-game transactions and asset transfers off-chain, reducing latency and transaction fees, and enabling smoother gameplay and more scalable gaming economies.

6. Benefits and Challenges

- **Advantages of Roll-ups**

  Scalability: Handle more transactions by processing them off-chain.

  Lower Costs: Reduce fees by batching transactions into a single on-chain submission.

  Speed: Increase transaction speed with quicker processing and finalisation.

  Security: Maintain strong security through cryptographic proofs and fraud prevention.

  Efficiency: Optimise resource use, minimising blockchain congestion and energy consumption.

- **Limitations and Challenges**
  - Rollups, while they borrow Ethereum's core security guarantees, still come with some risks relative to Ethereum's main net.
  - For one thing, a rollup's smart contracts can contain bugs – not unlike any other program built on Ethereum. While fail-safes and audits should help prevent exploits, relying on an external program to handle transactions will always carry some added risk.
  - Both types of rollups are also still in their infancy, and as such the networks on which they operate are often somewhat centralised. In some cases, the developing team behind a rollup maintains partial control over the network, and can theoretically pause or switch it off wherever they like.
  - Many roll-ups also continue to rely on centralised "sequencers" to efficiently coordinate transactions on the layer 2 chain. A sequencer can't spoof or alter transactions, but it could technically censor or re-order them to extract some benefit for itself.

7. Future Trends and Developments

- **Emerging Technologies and Innovations**
  - Upcoming advancements in Roll-ups technology.
- **Potential Market Impact**
  - Forecasts and predictions for future adoption and growth.
- **Challenges to Future Adoption**
  - Barriers to widespread adoption and possible solutions.

8. Case Study

- **Loopring**

  Overview: Loopring is a decentralised exchange (DEX) and payment protocol built on Ethereum. To overcome Ethereum's scalability issues, Loopring implemented zk-Rollups (Zero-Knowledge Rollups) to increase transaction throughput while maintaining security and reducing costs.

  How Loopring Uses zk-Rollups:

1. **Transaction Aggregation:**
   - **Process:** Loopring batches thousands of user transactions off-chain. These transactions include trades, transfers, and other operations.
   - **Benefit:** This batching significantly reduces the number of transactions that need to be processed on the Ethereum blockchain, lowering fees and reducing congestion.
2. **zk-SNARKs for Validation:**
   - **Process:** Each batch of transactions is validated using zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). A zk-SNARK is a cryptographic proof that allows Loopring to prove that the transactions in the batch are valid without revealing all the transaction details.
   - **Benefit:** This ensures that transactions are secure and accurate while preserving user privacy. The zk-SNARK proof is then submitted to Ethereum, where it is verified by a smart contract.
3. **On-Chain Finalization:**
   - **Process:** Once the proof is verified on-chain, all the transactions in the batch are finalised on the Ethereum blockchain.
   - **Benefit:** This method allows Loopring to maintain the security of the Ethereum network while vastly increasing transaction throughput—up to 2,025 trades per second, compared to Ethereum's 15-30 transactions per second.

  Benefits Achieved by Loopring:

1. **Scalability:**
   - Loopring can process a high volume of trades and transfers with zk-Rollups, allowing for a more scalable DEX that can compete with centralised exchanges in terms of speed.
2. **Lower Costs:**
   - Transaction fees are significantly reduced since only the zk-SNARK proof is recorded on-chain, rather than every individual transaction. Users pay a fraction of the fees they would on Layer 1 Ethereum.
3. **Security:**

    - Loopring inherits Ethereum's security while maintaining the privacy and integrity of user transactions through zk-SNARKs. This hybrid approach allows for decentralised, trustless transactions.
4. **User Experience:**
    - The use of zk-Rollups allows Loopring to offer a seamless and fast trading experience, with lower fees and faster transaction times, improving overall user satisfaction.

Real-World Impact:

- **Market Adoption:** Loopring has attracted a significant user base by providing an efficient, cost-effective, and secure platform for trading and payments. It serves as a model for other DEXs looking to scale on Ethereum.
- **Innovation:** Loopring's implementation of zk-Rollups has driven broader adoption of zk-Rollup technology within the Ethereum ecosystem, influencing other projects to explore similar solutions for scaling.

9. Conclusion

- **Summary of Findings**
    - Recap of the key points discussed.
- **Implications for the Industry**
    - How Roll-ups are expected to impact the industry.