

Zero-Knowledge for Privacy, Succinct for Rollups

Adrià Torralba-Agell^{1, 3}
atorralbaag@uoc.edu

Ghazaleh
Keshavarz^{2, 3}
ghazaleh.
keshavarzkalhor@uab.cat

Cristina
Pérez-Solà^{2, 3}
cperezsola@uoc.edu

David Megías^{1, 3}
dmegias@uoc.edu

¹Universitat Oberta de Catalunya

K-riptography and Information Security for Open Networks (KISON) Research Group

²Universitat Autònoma de Barcelona

SENDA - Security of Networks and Distributed Applications

³Cybercat - Center for Cybersecurity Research of Catalonia

April 24th, 2024



Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

Bitcoin and Ethereum do not scale



Slow



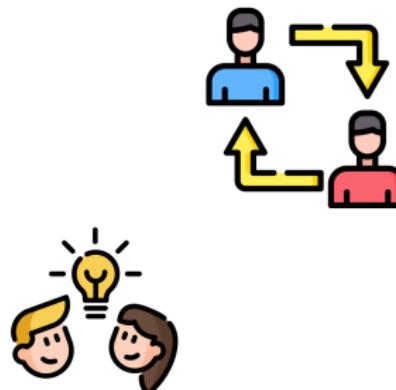
Expensive



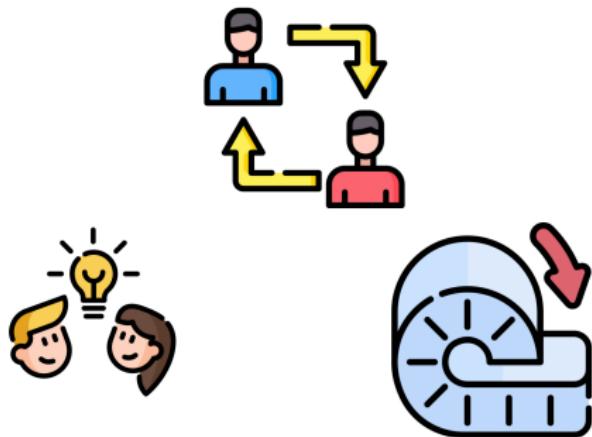
But people have ideas... Layer 2!



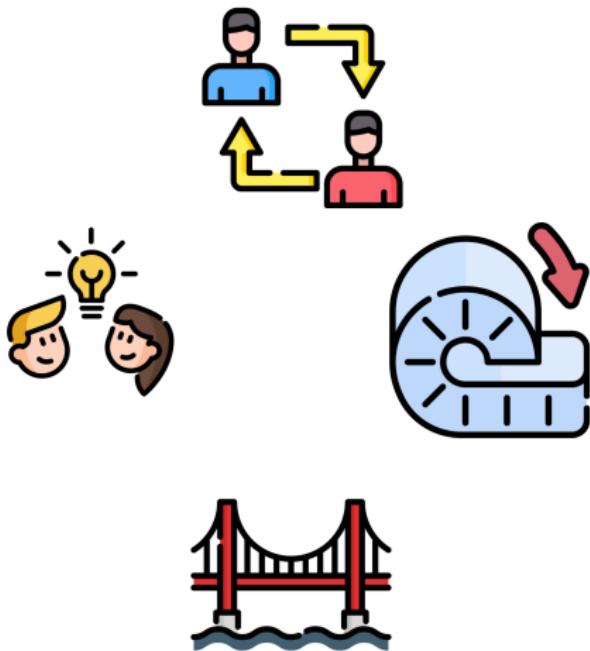
Payment Channel Networks



Rollups



Bridges to enable interoperability



We are interested on rollups

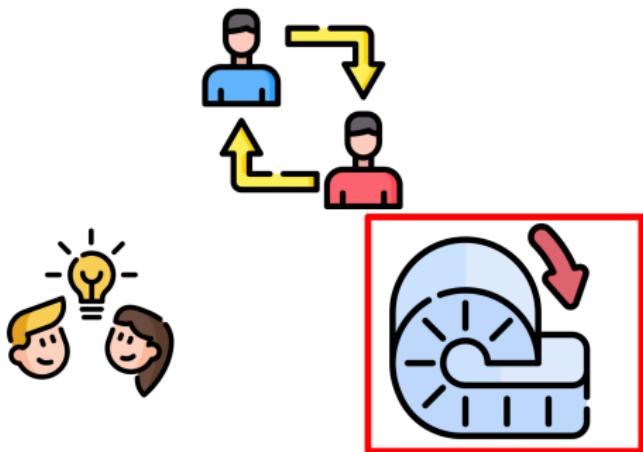


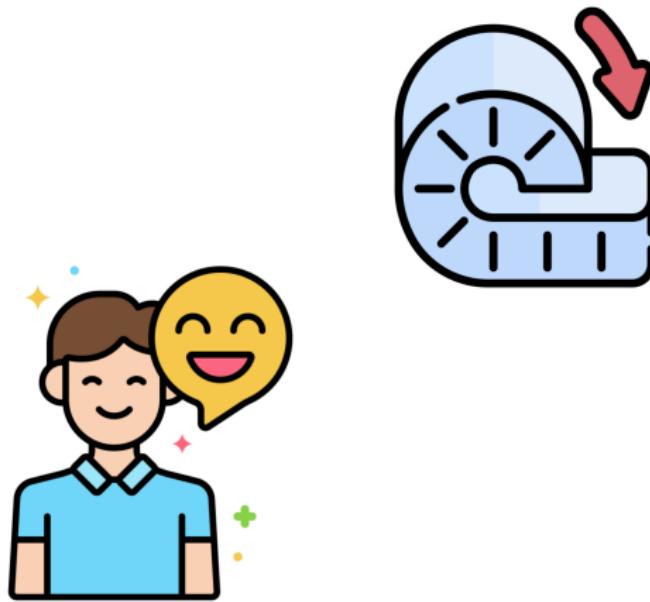
Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

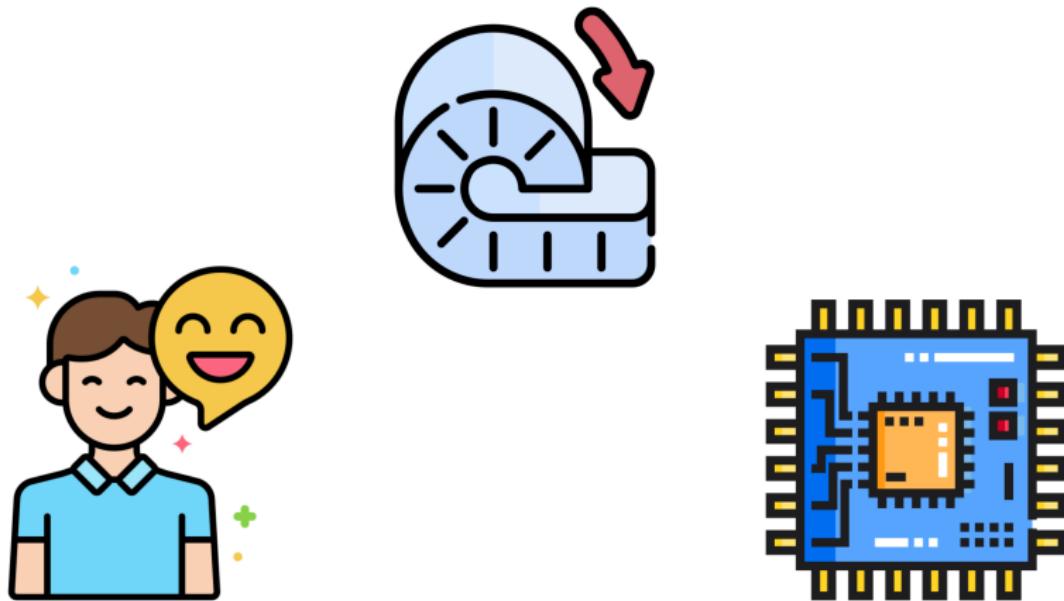
Rollups



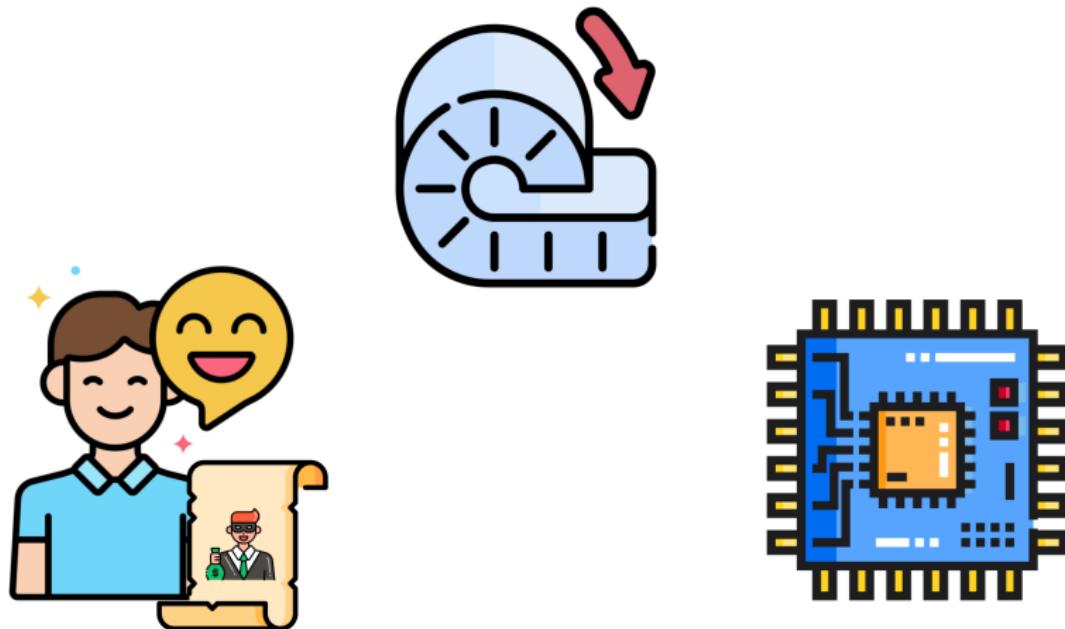
Optimistic Rollups



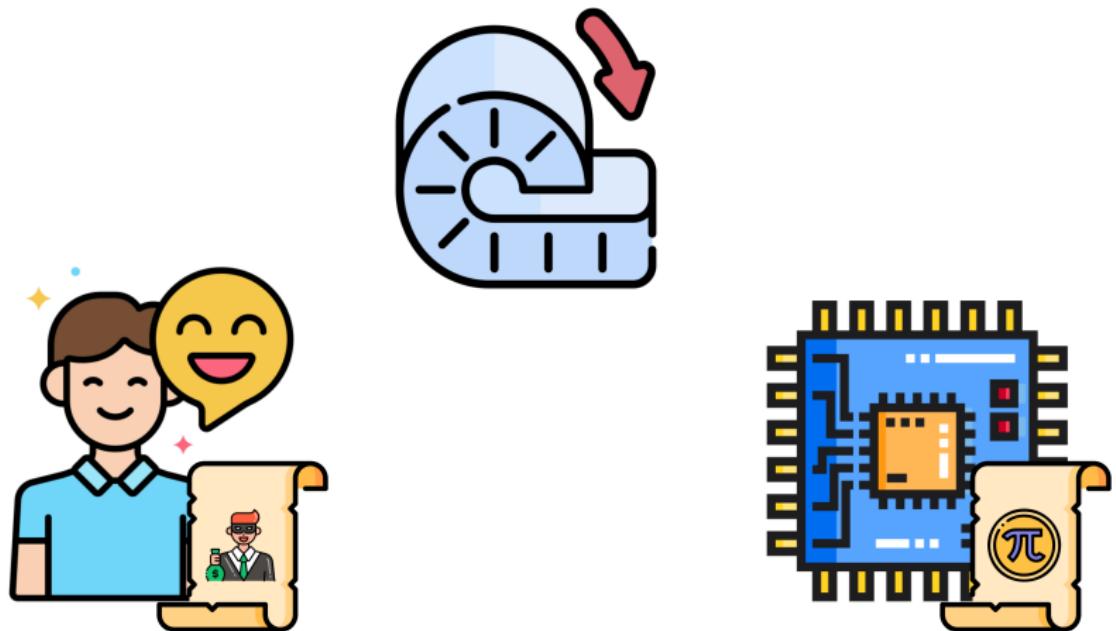
Zero-Knowledge Rollups



Optimistic Rollups - Fraud Proofs



Zero-Knowledge Rollups - Validity Proofs



Zero-Knowledge Rollups

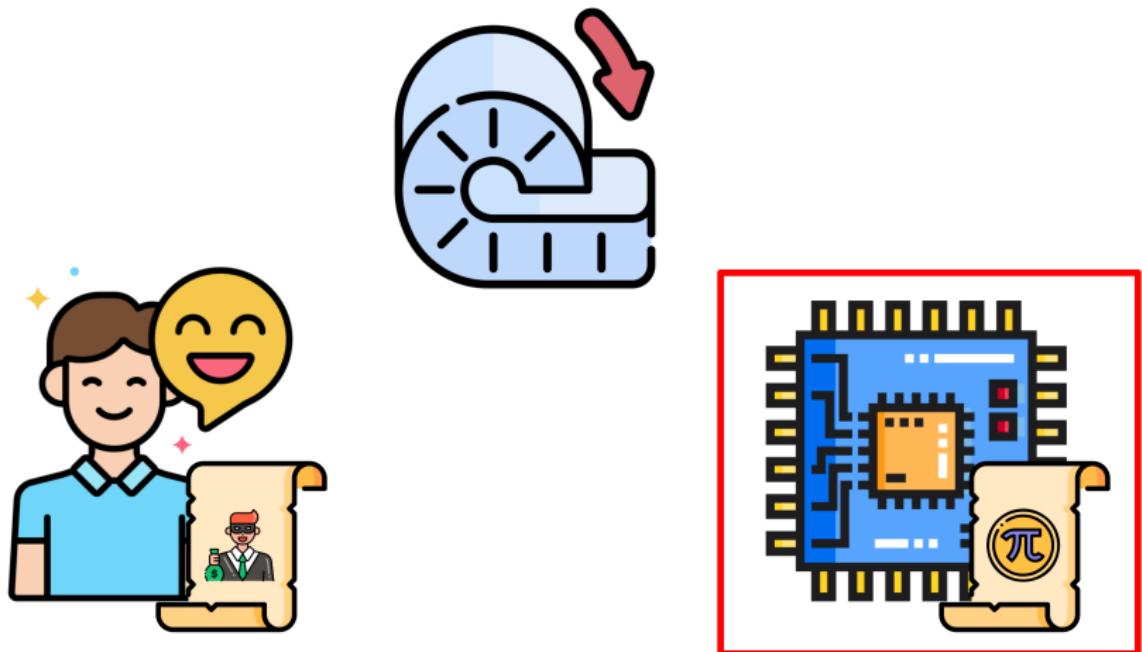


Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

Exploring a zkRollup...

 polygon zkEVM

Home Blockchain ▾ Tokens ▾ NFTs ▾ Resources ▾ Developers ▾ More ▾ | 

Transaction Details < >

[Overview](#) [State](#)

① Transaction Hash: 0x5f703426e8995dd9af7905a764835ba0dea53994e80d744906e9e7124d21c55 ⓘ

② Status:  Success

③ Block: 11872625 41 Block Confirmations

④ Timestamp: 2 mins ago (Apr 23 2024 03:10:39 PM +UTC)

⑤ Transaction Action: ➔ Transfer 0.02800000000000001 ETH To [0x5faF1212...A250D1F3f](#)

⑥ From: 0x5e09A85Aa1B2A9921ED010a4163745bb3e36284 ⓘ

⑦ To: 0x5faF1212B40b27669b2c0b8b5dFcB15A250D1F3f ⓘ

⑧ Value: ₿ 0.02800000000000001 ETH (\$90.62)

⑨ Transaction Fee: 0.000027576527328 ETH (\$0.09)

⑩ Effective Gas Price: 1.313167968 Gwei (0.00000001313167968 ETH)

⑪ Gas Limit & Usage by Txn: 34,650 | 21,000 (60.61%)

⑫ Gas Price: 1.837 Gwei

⑬ Other Attributes: Txn Type: 0 (Legacy) | Nonce: 20714 | Position In Block: 0

⑭ Input Data: 0x

More Details: [— Click to show less](#)

⑮ Private Note: To access the Private Note feature, you must be [Logged In](#)

ⓘ A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Exploring a zkRollup...

 polygon zkEVM

Home Blockchain ▾ Tokens ▾ NFTs ▾ Resources ▾ Developers ▾ More ▾ | 

Transaction Details < >

[Overview](#) [State](#)

① Transaction Hash: 0x5f703426e8995dd9af7905a764835ba0dea53994e80d744906e9e7124d21c55 ⓘ

② Status:  Success

③ Block: 11872625 41 Block Confirmations

④ Timestamp: 2 mins ago (Apr 23 2024 03:10:39 PM +UTC)

⑤ Transaction Action: Transfer 0.02800000000000001 ETH To [0x5faF1212...A250D1F3f](#)

⑥ From: [0x5e809A85Aa182A9921ED010a4163745bb3e36284](#) ⓘ

⑦ To: [0x5faF1212B40b27669b2c0b85dFc15A250D1F3f](#) ⓘ

⑧ Value: ₋ 0.02800000000000001 ETH (\$90.62)

⑨ Transaction Fee: 0.0000027576527328 ETH (\$0.09)

⑩ Effective Gas Price: 1.313167968 Gwei (0.00000001313167968 ETH)

⑪ Gas Limit & Usage by Txn: 34,650 | 21,000 (60.61%)

⑫ Gas Price: 1.837 Gwei

⑬ Other Attributes: [Txn Type: 0 \(Legacy\)](#) [Nonce: 20714](#) [Position In Block: 0](#)

⑭ Input Data: 0x

More Details: [— Click to show less](#)

⑮ Private Note: To access the Private Note feature, you must be [Logged In](#)

 A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Exploring a zkRollup...

 polygon zkEVM

Home Blockchain ▾ Tokens ▾ NFTs ▾ Resources ▾ Developers ▾ More ▾ | 

Transaction Details < >

[Overview](#) [State](#)

① Transaction Hash: [0x53f703426e8995dd9af7905a764835ba0dea53994e80d744906e9e7124d21c55](#) ⓘ

② Status:  Success

③ Block: [11872625](#) 41 Block Confirmations

④ Timestamp: 2 mins ago (Apr 23 2024 03:10:39 PM +UTC)

⑤ Transaction Action: Transfer 0.02800000000000001 ETH To [0x5faF1212...A250D1F3f](#)

⑥ From: [0x5e809A85Aa182A9921ED010a4163745bb3e36284](#) ⓘ

⑦ To: [0x5faF1212B40b27669b2c0b8b5dFc15A250D1F3f](#) ⓘ

⑧ Value: ₋ 0.02800000000000001 ETH (\$90.62)

⑨ Transaction Fee: 0.0000027576527328 ETH (\$0.09)

⑩ Effective Gas Price: 1.313167968 Gwei (0.000000001313167968 ETH)

⑪ Gas Limit & Usage by Txn: 34,650 | 21,000 (60.61%)

⑫ Gas Price: 1.837 Gwei

⑬ Other Attributes: Txn Type: 0 (Legacy) | Nonce: 20714 | Position In Block: 0

⑭ Input Data: 0x

More Details: [— Click to show less](#)

⑮ Private Note: To access the Private Note feature, you must be [Logged In](#)

ⓘ A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Exploring a zkRollup...

 **polygon zkEVM**

Home Blockchain ▾ Tokens ▾ NFTs ▾ Resources ▾ Developers ▾ More ▾ | 

Transaction Details < >

Overview State

① Transaction Hash: 0x53f703426e8995dd9af7905a764835ba0dea53994e80d744906e9e7124d21c55 ⓘ

② Status:  Success

③ Block: 11872625 41 Block Confirmations

④ Timestamp: 2 mins ago (Apr 23 2024 03:10:39 PM +UTC)

⑤ Transaction Action: ➔ Transfer 0.02800000000000001 ETH To [0x5faF1212...A250D1F3f](#)

⑥ From: 0x5e809A85Aa1B2A9921ED010a4163745bb3e36284 ⓘ

⑦ To: 0x5faF1212B40b27669b2c0b8b5dFc15A250D1F3f ⓘ

⑧ Value: ₋ 0.02800000000000001 ETH (\$90.62)

⑨ Transaction Fee: 0.000027576527328 ETH (\$0.09)

⑩ Effective Gas Price: 1.313167968 Gwei (0.00000001313167968 ETH)

⑪ Gas Limit & Usage by Txn: 34,650 | 21,000 (60.61%)

⑫ Gas Price: 1.837 Gwei

⑬ Other Attributes: Txn Type: 0 (Legacy) | Nonce: 20714 | Position In Block: 0

⑭ Input Data: 0x

More Details: — Click to show less

⑮ Private Note: To access the Private Note feature, you must be [Logged In](#)

ⓘ A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Exploring a zkRollup...

 [polygon zkEVM](#)

[Home](#) [Blockchain](#) [Tokens](#) [NFTs](#) [Resources](#) [Developers](#) [More](#) | [Sign In](#)

Transaction Details < >

[Overview](#) [State](#)

① Transaction Hash: [0x5f703426e8995dd9af7905a764835ba0dea53994e80d744906e9e7124d21c55](#)

② Status: Success

③ Block: [11872625](#) 41 Block Confirmations

④ Timestamp: [2 mins ago \(Apr 23 2024 03:10:39 PM +UTC\)](#)

⑤ Transaction Action: [Transfer 0.02800000000000001 ETH To \[0x5faF1212...A250D1F3f\]\(#\)](#)

⑥ From: [0x5e809A85Aa1B2A9921ED010a4163745bb3e36284](#)

⑦ To: [0x5faF1212B40b27669b2c0b8b5dFc15A250D1F3f](#)

⑧ Value: [0.02800000000000001 ETH \(\\$90.62\)](#)

⑨ Transaction Fee: [0.0000027576527328 ETH \(\\$0.09\)](#)

⑩ Effective Gas Price: [1.313167968 Gwei \(0.000000001313167968 ETH\)](#)

⑪ Gas Limit & Usage by Txn: [34,650](#) | [21,000 \(60.61%\)](#)

⑫ Gas Price: [1.837 Gwei](#)

⑬ Other Attributes: Txn Type: 0 [Legacy] | Nonce: 20714 | Position In Block: 0

⑭ Input Data: [0x](#)

More Details: [— Click to show less](#)

⑮ Private Note: [To access the Private Note feature, you must be Logged In](#)

⚠ A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

SNARKs

SNARKs

S Succinct

SNARKs

S Succinct: “means that the Proof is short.”

SNARKs

S Succinct: “means that the Proof is short.”

N Non-interactive

SNARKs

- S Succinct: “means that the Proof is short.”
- N Non-interactive: “means that the Proof is ‘static’, consisting of a single message from the Prover.”

SNARKs

S Succinct: “means that the Proof is short.”

N Non-interactive: “means that the Proof is ‘static’, consisting of a single message from the Prover.”

AR ARguments

SNARKs

- S Succinct: “means that the Proof is short.”
- N Non-interactive: “means that the Proof is ‘static’, consisting of a single message from the Prover.”
- AR ARguments: “ensures protection for the Verifier against a computationally bounded Prover.”

SNARKs

- S Succinct: “means that the Proof is short.”
- N Non-interactive: “means that the Proof is ‘static’, consisting of a single message from the Prover.”
- AR ARguments: “ensures protection for the Verifier against a computationally bounded Prover.”
- K of Knowledge

SNARKs

- S Succinct: “means that the Proof is short.”
- N Non-interactive: “means that the Proof is ‘static’, consisting of a single message from the Prover.”
- AR ARguments: “ensures protection for the Verifier against a computationally bounded Prover.”
- K of Knowledge: “means that the protocol establishes not only that the statement is true, but also that the Prover *knows* a ‘witness’.”

SNARKs

- S Succinct:** “means that the Proof is short.”
- N Non-interactive:** “means that the Proof is ‘static’, consisting of a single message from the Prover.”
- AR ARguments:** “ensures protection for the Verifier against a computationally bounded Prover.”
- K of Knowledge:** “means that the protocol establishes not only that the statement is true, but also that the Prover *knows* a ‘witness’.”

Renaming zkRollups

sucRollup Succinct Rollup?

Renaming zkRollups

sucRollup Succinct Rollup?

ivcRollup IncrementallyVerifiableComputation Rollup?

Renaming zkRollups

sucRollup Succinct Rollup?

ivcRollup IncrementallyVerifiableComputation Rollup?

Or... Rollup + Privacy

Renaming zkRollups

sucRollup Succinct Rollup?

ivcRollup IncrementallyVerifiableComputation Rollup?

Or... Rollup + Privacy

zkzkRollup Zero-Knowledge(Zero-Knowledge Rollup)?

Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

Original classification



vitalik.eth ✅

@VitalikButerin

suggests "validium" as a clearer name for plasma-with-snarks (aka zk rollup but with offchain data). That is:
pic.twitter.com/lGB2MMrXp0

	SNARKs/ STARKs	Fraud proofs
Data on-chain	ZK rollup	Optimistic rollup
Data off-chain	Validium	Plasma



Eli
Ben-
Sasson

@@EliBenSasson · Jun
1

@avihu28 @VitalikButerin @StarkWareLtd
@reddit @ethereum @fuellabs_ Suggest
"Validia" for this class of protocols, like
plasma in having data offchain, like zk-rollups
in being validity proofs. (Thanks,
@VitalikButerin for Latin spelling help :-)

3:58 PM · June 1, 2020

44 Retweets 192 Likes

New classification



cal (zk/acc) 
@calummoore

sorry, but this is what the table should actually be

pic.twitter.com/w7Q64RQG40

	SNARKs/ STARKs	Fraud proofs
Data  Public	ZK-rollup succinct rollup	Optimistic rollup
Data  Private	Validium zk-rollup	Plasma impossible



vitalik.eth @@VitalikButerin · Jun 1

@EliBenSasson suggests "validium" as a clearer name for plasma-with-snarks (aka zk rollup but with offchain data). That is:
pic.twitter.com/lGB2MMrXp0x.com/EliBenSasson/s...

7:00 PM · April 18, 2024

1 Retweet 6 Likes

Table of Contents

- 1 Why do we need Layer 2s (and, in particular, rollups)?
- 2 Optimistic and Zero-Knowledge Rollups
- 3 Exploring a zkRollup
- 4 SNARKs
- 5 New trends
- 6 Adding Privacy to rollups
- 7 Conclusions

SNARKs

S Succinct

N Non-interactive

AR ARguments

K of Knowledge

(zk)SNARKs

(zk) Zero-Knowledge \Rightarrow as a way to enable Privacy

S Succinct

N Non-interactive

AR ARguments

K of Knowledge

Adding Privacy to Rollups

From Satybaldy et al. (2020)

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing
- Ring Signatures

Adding Privacy to Rollups

From Satybalay et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing
- Ring Signatures
- Differential Privacy

Adding Privacy to Rollups

From Satybalay et al. (2020)

- **Zero-Knowledge Proofs (zkSNARK or zkSTARK)**
- Secure Multi-party Computation
- **Homomorphic Encryption**
- **Commitment Schemes**
- Mixing
- Ring Signatures
- Differential Privacy

Conclusions

- Next steps for zkRollups (after decentralisation)



Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that



Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that
 - ▶ Aztec: “Privacy-first L2 on Ethereum”



Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that
 - ▶ Aztec: “Privacy-first L2 on Ethereum”
 - ▶ Payy (but UTXO-based...)



Thank you for your attention!



@0xAdriaTorralba



0xAdriaTorralba



atorralbaag@uoc.edu



QR Code to my research

