

A Taxonomy of Security Analysis of Blockchain Layer 2 Scalability Solutions and Future Directions

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

Cristina Pérez-Solà^{2, 3}
cperezsola@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 19th, 2024



Table of Contents

- 1 Why does Layer 1 not scale?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Table of Contents

- 1 Why does Layer 1 not scale?
 - Blockchain Trilemma
 - A little bit of history on reaching consensus
 - What does this have to do with blockchains?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Blockchain Trilemma

- 3 desirable properties
 - ▶ Scalability
 - ▶ Security
 - ▶ Decentralization
- Vitalik Buterin (and other authors) claim that all 3 are **incompatible** at the **same time**
 - ▶ Blockchain Trilemma

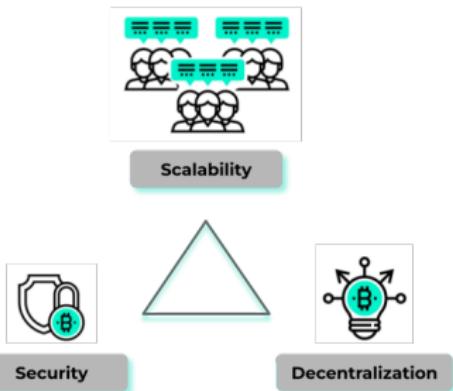


Figure: Diagram of the Blockchain Trilemma

A little bit of history on reaching consensus on a decentralised network

1977 Lamport presented a framework for proving the correctness of a multi-process program.

- ▶ Safety,
- ▶ Liveness.

1980 Pease et al. formally defined an algorithm to reach consensus with faulty (or malign) parties in the system.

1985 Fisher et al. presented the FLP (Fisher, Lynch, Paterson) impossibility.

- ▶ Agreement,
- ▶ Validity,
- ▶ Termination.

1999 Brewer presented the **CAP conjecture**.

- ▶ Consistency,
- ▶ Availability,
- ▶ Partition-tolerance.

2002 Gilbert and Lynch proved the conjecture: **CAP theorem**.

What does this have to do with blockchain?

- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,

What does this have to do with blockchain?

- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,
 - ▶ **Consistency,**

What does this have to do with blockchain?

- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,
 - ▶ **Consistency**,
 - ▶ **Availability**.

What does this have to do with blockchain?

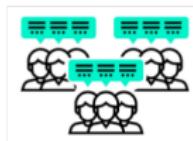
- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,
 - ▶ **Consistency**,
 - ▶ **Availability**.
- It **might be possible** to relate

CAP theorem \iff Blockchain trilemma

What does this have to do with blockchain?

- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,
 - ▶ **Consistency**,
 - ▶ **Availability**.
- It **might be possible** to relate

CAP theorem \iff Blockchain trilemma



Scalability



Security



Decentralization

Thank you for your attention!

Directed by
ROBERT B. WEIDE

Table of Contents

- 1 Why does Layer 1 not scale?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Bitcoin and Ethereum do not scale



Slow



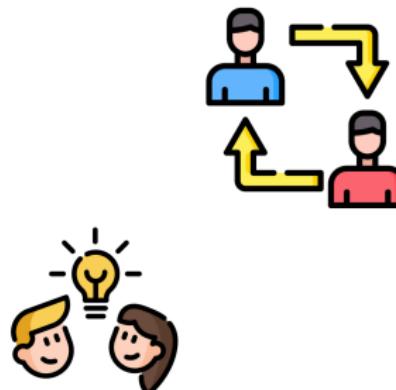
Expensive



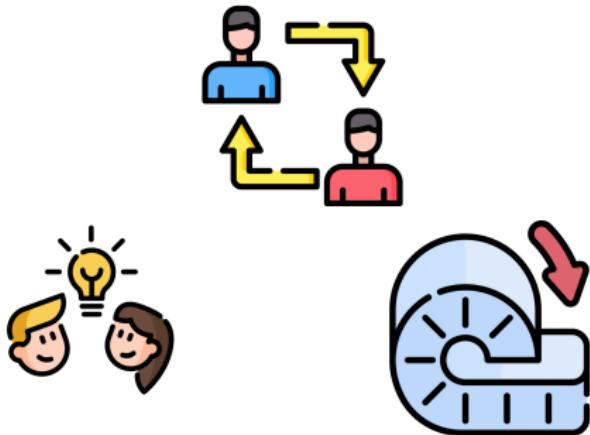
But people have ideas... Layer 2!



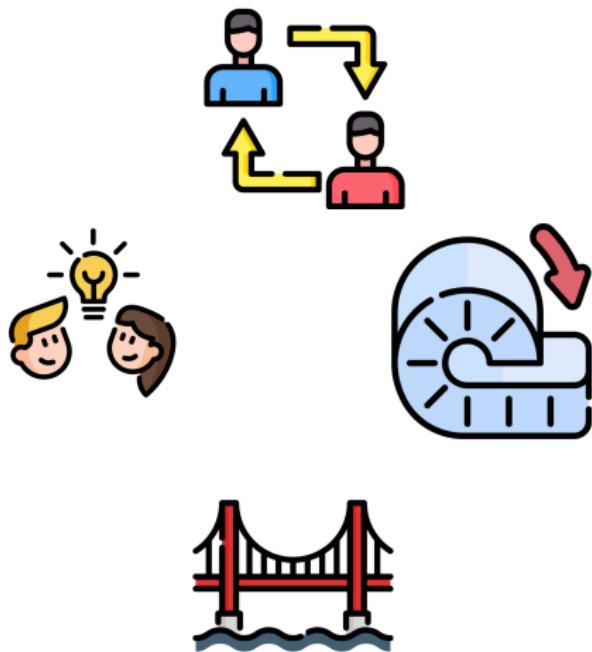
Payment Channel Networks



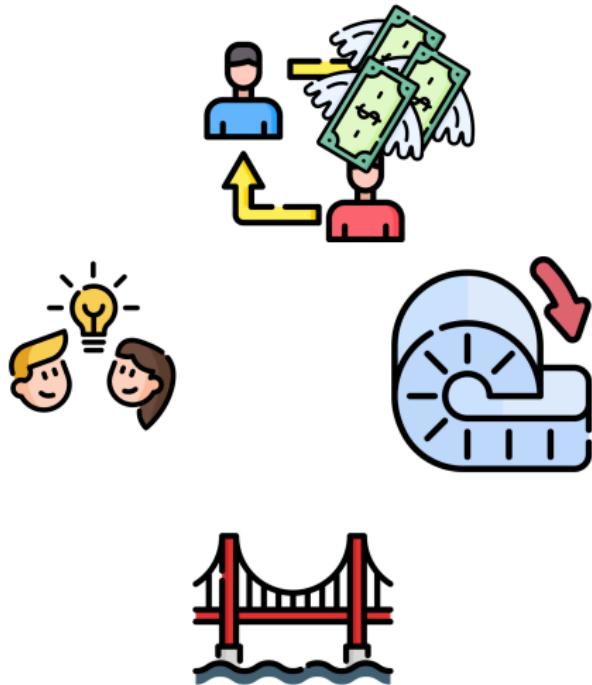
Zero-Knowledge Rollups and Optimistic Rollups



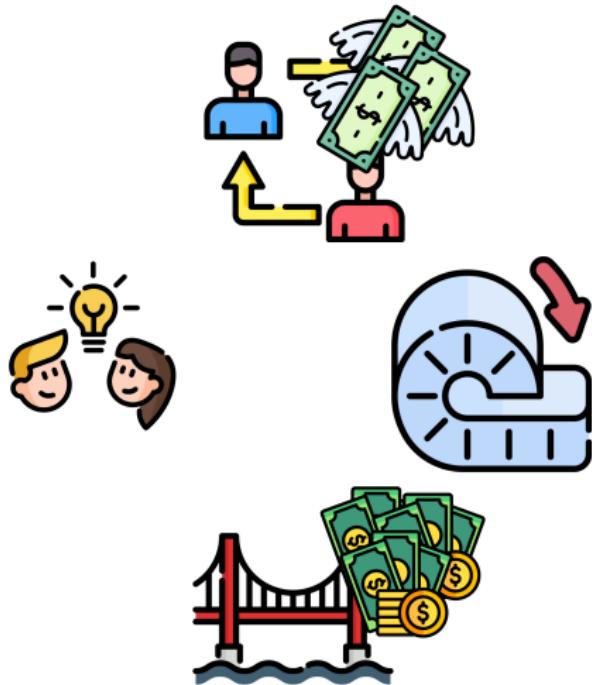
Bridges to enable interoperability



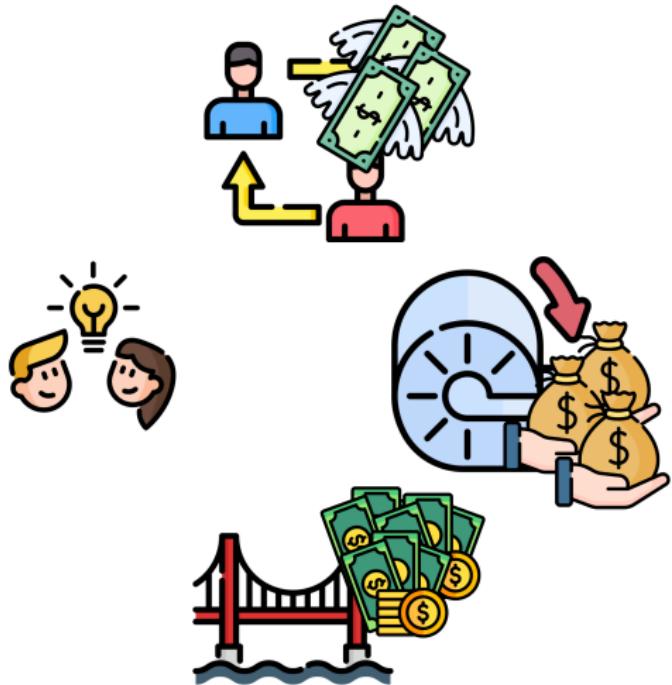
Money



More money...



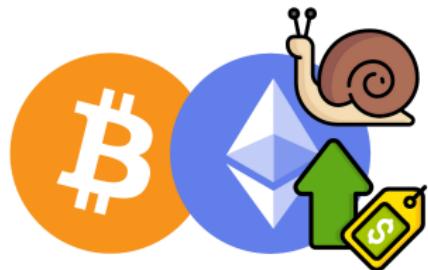
Even more money



So... everybody is happy :)



So... everybody is happy :)



So... everybody is happy :)... Right?



Table of Contents

- 1 Why does Layer 1 not scale?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Why do we need this Survey?



T&C | leaderboard | dark | env

1. Ronin Network - REKT Unaudited \$624,469,466 03/23/2022	24. Woofs - Rekt Certik \$45,000,000 03/05/2024	47. Spartan Protocol - REKT M/A \$50,500,000 05/02/2021	70. Inverse Finance - REKT Unaudited \$15,600,000 04/02/2022	93. Visor Finance - REKT Unaudited \$8,246,000 12/21/2021
2. Poly Network - REKT Unaudited \$611,000,000 06/12/2021	25. Orbit Bridge - REKT Out of scope \$81,500,000 12/15/2022	48. Grim Finance - REKT Solidity Finance \$26,000,000 12/15/2021	71. Esinence - Rekt in prod Unaudited \$15,000,000 09/28/2020	94. THORChain - REKT 2 THORChain \$0,000,000 07/22/2021
3. BNB Bridge - REKT Unaudited \$598,000,000 10/09/2022	26. Fei Hari - REKT Unaudited \$80,000,000 05/01/2022	49. Deribit - REKT N/A \$28,000,000 11/01/2022	72. Furucombo - REKT Unaudited \$14,000,000 02/27/2021	95. Hack Epidemic (Orgi - REKT) Unaudited \$8,000,000 11/17/2020
4. SBF - MASK OFF N/A \$477,000,000 11/17/2022	27. Qubit Finance - REKT Unaudited \$46,000,000 01/28/2022	50. Wintermute - REKT N/A \$27,400,000 06/05/2022	73. Deus DAO - REKT 2 Armor Labs \$13,000,000 04/28/2022	96. LCK - REKT Unaudited \$7,948,000 01/08/2022
5. Wormhole - REKT Hesdyne \$223,000,000 02/02/2022	28. Ascendex - REKT Unaudited \$77,700,000 12/12/2021	51. StableMagnet - REKT Techrate \$27,000,000 04/23/2021	74. Compounder Finance - REKT out of scope \$12,000,000 02/28/2020	97. HTX (Hub) - REKT N/A \$7,980,000 09/24/2023
6. Mixin Network - REKT N/A \$200,000,000 09/23/2022	29. Curve, Vyper - REKT N/A \$49,300,000 07/20/2023	52. Paid Network - REKT Unaudited \$27,000,000 04/05/2021	75. Agave DAO, Hundred - REKT Unaudited \$11,700,000 03/15/2022	98. Anyswap - REKT Unaudited \$7,980,000 07/10/2021
7. Euler Finance - REKT Sherlock \$197,000,000 03/13/2023	30. Munchables - REKT Entersafe \$21,000,000 05/26/2024	53. Kronos Research - REKT N/A \$26,000,000 11/18/2023	76. PrimalFi - REKT PrimalFi \$11,000,000 05/28/2024	99. Warp Finance - REKT Hacken \$7,000,000 12/18/2020
8. BitMart - REKT N/A \$194,000,000 12/08/2021	31. AlphaPro - REKT M/A \$44,000,000 09/22/2023	54. Harvest Finance - REKT Haechi, Peskashield \$26,000,000 10/26/2020	77. Yearn - REKT 2 Unaudited \$11,000,000 04/13/2023	100. Meter - REKT Unaudited \$7,700,000 02/06/2022
9. Nomad Bridge - REKT N/A \$190,000,000 08/07/2022	32. EasyFI - REKT Unaudited \$51,000,000 04/19/2021	55. AnkR & Helio - REKT N/A \$24,000,000 12/02/2022	78. Saddle Finance - REKT 2 Unaudited \$11,000,000 12/02/2021	101. Nightmare on Street M/A \$7,500,000 10/17/2023
10. Beanstalk - REKT Unaudited \$181,000,000 04/17/2022	33. Uranium Finance - REKT Unaudited \$57,200,000 04/28/2021	56. Xtokens - REKT Peckshield \$20,000,000 05/17/2021	79. ValueDefi - REKT 3 Unaudited \$11,000,000 05/07/2021	102. Jumbo's Protocol - REKT Unaudited \$7,500,000 05/20/2023
11. Wintermute - REKT 2 N/A \$162,100,000 09/28/2022	34. b2x - REKT Unaudited \$16,000,000 11/05/2021	57. BALD on Base - REKT N/A \$23,000,000 07/01/2023	80. Yearn - REKT Unaudited \$11,000,000 02/05/2021	103. Hundred Finance - REKT 2 #whiteHabD40 \$7,400,000 04/15/2023
12. Compound - REKT Unaudited \$167,000,000 08/07/2021	35. CoinEx - REKT N/A \$14,500,000 09/12/2023	58. Elephant Finance - REKT Solidity Finance \$22,200,000 04/11/2021	81. Degen Finance - REKT Peckshield \$10,000,000 02/18/2022	104. Exactly Protocol - REKT Out of scope \$7,200,000 08/18/2023
13. Vulcan Forged - REKT Unaudited \$148,000,000 12/13/2021	36. KyberSwap - REKT ChainSecurity, Sherlock \$44,000,000 11/22/2023	59. Blitz Finance, Venu Protocol - REKT n/a \$21,000,000 05/13/2022	82. Arbix Finance - REKT Certik \$11,000,000 01/04/2022	105. BurgerSwap - REKT Unaudited \$7,200,000 05/20/2021
14. Cream Finance - REKT 2 Unaudited \$139,000,000 10/27/2021	37. Cashio - REKT Unaudited \$48,000,000 05/23/2022	60. Transmit Swap - REKT Out of scope \$21,200,000 10/09/2022	83. Rari Capital - REKT Quantstamp \$10,000,000 05/08/2021	106. ValueDefi - REKT Unaudited \$7,000,000 11/14/2023
15. Multichain - REKT 2 N/A \$119,300,000 07/09/2023	38. PancakeBunny - REKT Unaudited \$45,000,000 05/19/2021	61. Unizen - Rekt Helborn, Verichains \$21,000,000 01/09/2024	84. ValueDefi - REKT 2 Unaudited \$10,000,000 05/05/2021	107. Abracadabra - REKT Unaudited \$6,500,000 01/30/2024
16. Poloniex - REKT N/A \$116,000,000 11/14/2023	39. Kueccin - REKT Internal audit \$45,000,000 09/19/2028	62. Popsicle Finance - REKT Peckshield \$20,000,000 04/03/2021	85. Cover - REKT Arcadia Group \$11,000,000 12/24/2024	108. Deus DAO - REKT Unaudited \$6,500,000 03/05/2023
17. SongDAO - REKT Out of scope \$120,000,000 08/01/2023	40. Stake - REKT N/A \$11,000,000 09/04/2023	63. Pickle Finance - REKT Unaudited \$19,700,000 11/22/2020	86. dydx - REKT N/A \$9,000,000 11/18/2023	109. Lodestar Finance - REKT Unaudited \$6,500,000 12/18/2022
18. Badger - REKT Unaudited \$120,000,000 12/07/2021	41. Alpha Finance - REKT Quantstamp, Peckshield \$37,500,000 02/13/2021	64. Cream Finance - REKT Unaudited \$18,000,000 09/20/2021	87. Punk Protocol - REKT Unaudited \$8,000,000 08/19/2021	110. Alchemix - REKT Unaudited \$6,500,000 09/16/2021
19. Mango Markets - REKT Out of Scope \$111,000,000 10/17/2022	42. LastPass Users - REKT N/A \$37,000,000 12/14/2022	65. Snodog - REKT Unaudited \$18,100,000 11/25/2021	88. Safemoon - REKT Unaudited \$8,000,000 09/23/2023	111. Seneca Protocol - REKT Helborn \$6,400,000 02/28/2024
20. Atomic Wallet - REKT Unaudited \$100,000,000 06/03/2022	43. Yee Finance - REKT Elminist \$34,000,000 09/21/2021	66. b2barn - REKT Unaudited \$18,000,000 05/17/2021	89. Cress Finance - REKT Drama Systems \$8,000,000 07/03/2022	112. Belt - REKT Hesdyne \$6,300,000 03/29/2021
21. Harmony Bridge - REKT N/A \$101,000,000 06/23/2022	44. Crypto.y - REKT Deelitze \$33,700,000 01/18/2022	67. Curio - REKT N/A \$16,000,000 03/23/2024	90. Superfluid - REKT Peckshield \$6,700,000 02/08/2022	113. Audius - REKT Kloudzki, OpenZeppelin \$6,000,000 07/23/2022
22. MEV Bridge - REKT N/A \$99,100,000 11/22/2023	45. Meerkat Finance - REKT B2B - REKT Unaudited \$31,000,000 05/04/2021	68. IndexFinance - REKT Unaudited \$16,000,000 10/14/2021	91. Platypus Finance - REKT Unaudited \$6,500,000 02/17/2023	114. Bodhi - REKT Unaudited \$5,900,000 07/15/2025
23. Mirror Protocol - REKT Unaudited \$92,400,000 10/08/2021	46. Monet - REKT Helborn, Peckshield \$31,000,000 11/08/2021	69. Team Finance - REKT Tokio Security \$15,600,000 10/27/2022	92. Moala Market - REKT Aava \$8,400,000 10/19/2022	115. Inverse Finance - REKT 2 Unaudited \$5,800,000 04/16/2022

Why do we need this Survey?



T&C | leaderboard | dark | en

1. Ronin Network - REKT Unaudited \$624,000,000 03/23/2022	24. Woofi - Rekt Cerik \$85,000,000 03/05/2024	47. Spartan Protocol - REKT N/A \$20,500,000 05/02/2021	70. Inverse Finance - REKT Unaudited \$15,600,000 04/02/2022	93. Visor Finance - REKT Unaudited \$8,200,000 12/21/2021
2. Poly Network + REKT Unaudited \$651,000,000 08/07/2023	25. Orbit Bridge - REKT Out of scope \$81,500,000 12/18/2023	48. Grim Finance - REKT Solidity Finance \$20,000,000 11/01/2022	71. Eminence - Rekt Prod Unaudited \$15,000,000 09/28/2020	94. THORChain - REKT 2 THORChain \$8,000,000 07/22/2021
3. BNB Bridge - REKT Unaudited \$598,000,000 10/09/2022	26. Fed Rari - REKT 2 Unaudited \$81,000,000 05/01/2022	49. Deribit - REKT N/A \$20,000,000 11/01/2022	72. FurcioCom - REKT Unaudited \$14,000,000 02/27/2021	95. Hack Epidemic (Orgi - REKT) Unaudited \$8,000,000 11/17/2020
4. SBF - MASK OFF N/A \$477,000,000 11/17/2022	27. Qubit Finance - REKT Unaudited \$81,000,000 01/28/2022	50. Wintermute - REKT N/A \$27,400,000 04/05/2022	73. Deus DAO - REKT 2 Armor Labs \$13,400,000 04/08/2022	96. LCK - REKT Unaudited \$7,940,000 01/08/2022
5. Kornhole - REKT ReadyMe \$323,000,000 02/02/2022	28. Ascendex - REKT Unaudited \$77,700,000 12/12/2021	51. StableMagnet - REKT Techrate \$27,000,000 09/23/2021	74. Compound Finance - REKT out of scope \$12,000,000 12/02/2022	97. HTX (Hub) - REKT N/A \$7,900,000 03/24/2023
6. Mixin Network - REKT N/A \$269,000,000 09/23/2023	29. Curve, Vyper - REKT N/A \$89,500,000 07/06/2023	52. Paid Network - REKT Unaudited \$27,000,000 05/05/2021	75. Agave DAO, Hundred - REKT Unaudited \$11,700,000 05/15/2022	98. Anyswap - REKT Unaudited \$7,900,000 07/16/2021
7. Euler Finance - REKT Sherlock \$197,000,000 08/23/2023	30. Munchables - REKT Entersaf \$42,500,000 05/24/2024	53. Kronos Finance - REKT N/A \$20,400,000 11/11/2023	76. Primalis - REKT PrismFi \$11,600,000 05/28/2024	99. Warp Finance - REKT Haken \$7,800,000 12/18/2020
8. BitMart - REKT N/A \$191,000,000 12/07/2023	31. AlphaPro - REKT N/A \$64,000,000 07/22/2023	54. Harvest Finance - REKT Haschi, Peckshield \$25,000,000 10/26/2020	77. Years - REKT 2 Unaudited \$11,400,000 04/13/2023	100. Meter - REKT Unaudited \$7,700,000 02/06/2020
9. Homad Bridge - REKT N/A \$191,000,000 08/07/2022	32. EasyFI - REKT Unaudited \$59,000,000 04/19/2021	55. Ankr & Holo - REKT N/A \$24,000,000 12/02/2022	78. Saddle Finance - REKT 2 Unaudited \$11,000,000 12/02/2021	101. Nightfang on FTN Street N/A \$7,500,000 10/17/2020
10. Beanztall - REKT Unaudited \$181,400,000 04/17/2022	33. Uranium Finance - REKT Unaudited \$57,200,000 04/28/2021	56. Xtokens - REKT Peckshield \$24,000,000 05/12/2021	79. Value Defi - REKT 3 Unaudited \$11,000,000 05/07/2021	102. Jisho's Protocol - REKT Unaudited \$7,500,000 05/28/2023
11. Wintermute - REKT 2 N/A \$162,300,000 04/02/2022	34. b2x - REKT Unaudited \$55,000,000 11/05/2021	57. BALD on Base - REKT N/A \$22,000,000 07/31/2023	80. Years - REKT Unaudited \$11,000,000 02/05/2021	103. Hundred Finance - REKT 2 WhitehatDAO \$7,400,000 04/15/2023
12. Compound - REKT Unaudited \$147,000,000 09/23/2023	35. CoinEx - REKT N/A \$50,000,000 09/12/2023	58. Elephant Money - REKT Solidity Finance \$22,200,000 04/17/2021	81. Dego Finance - REKT Peckshield \$10,000,000 02/18/2022	104. Exactly Protocol - REKT Out of scope \$7,200,000 08/18/2020
13. Vulcan Forged - REKT Unaudited \$148,000,000 12/13/2021	36. KyberSwap - REKT ChainSecurity, Sherlock \$44,000,000 11/22/2023	59. Blizz Finance, Venus Protocol - REKT N/A \$21,600,000 05/13/2022	82. Arbitx Finance - REKT CertiK \$10,000,000 01/04/2022	105. BurgerSwap - REKT Unaudited \$7,200,000 05/28/2021
14. Cray Finance - REKT 2 Unaudited \$134,000,000 10/27/2021	37. Cashio - REKT Unaudited \$48,000,000 03/23/2023	60. Transmit Swap - REKT Out of scope \$21,200,000 10/08/2022	83. Rari Capital - REKT Quantstamp \$10,000,000 05/04/2021	106. Value Defi - REKT Unaudited \$7,000,000 11/14/2020
15. Multichain - REKT 2 N/A \$120,300,000 07/09/2023	38. PancakeBunny - REKT Unaudited \$45,000,000 05/19/2021	61. Unizen - Rekt Helborn, Verchaine \$21,000,000 03/08/2024	84. Value Defi - REKT 2 Unaudited \$10,000,000 05/05/2021	107. Abracadabra - REKT Unaudited \$6,300,000 01/30/2024
16. Polonex - REKT N/A \$179,000,000 11/19/2023	39. Kucoin - REKT Internal audit \$45,000,000 09/29/2028	62. Popcycle Finance - REKT Peckshield \$20,000,000 05/05/2021	85. Cover - REKT Arcadia Group \$9,400,000 12/29/2028	108. Deus DAO - REKT Unaudited \$6,300,000 05/05/2023
17. BongDAO - REKT Out of scope \$129,000,000 02/01/2023	40. Stake - REKT N/A \$41,600,000 09/04/2023	63. Pickle Finance - REKT Unaudited \$19,700,000 11/18/2020	86. dYdX - REKT N/A \$9,000,000 11/18/2023	109. Lodestar Finance - REKT Unaudited \$6,300,000 12/10/2022
18. Badger - REKT Unaudited \$129,000,000 12/02/2021	41. Alpha Finance - REKT Quantstamp, Peckshield \$37,500,000 02/13/2021	64. Creas Finance - REKT Unaudited \$18,000,000 05/26/2021	87. Punkt Protocol - REKT Unaudited \$8,500,000 06/17/2021	110. Alchemix - REKT Unaudited \$6,300,000 05/16/2021
19. Mango Markets - REKT Out of Scope \$111,400,000 10/17/2022	42. LastPass Users - REKT N/A \$37,000,000 12/14/2022	65. Snowdog - REKT Unaudited \$18,100,000 11/25/2021	88. Safemoon - REKT Unaudited \$8,000,000 05/28/2023	111. Seneca Protocol - REKT Halborn \$6,400,000 02/28/2024
20. Atomic Wallet - REKT Unaudited \$100,400,000 04/05/2023	43. Vee Finance - REKT Element \$34,000,000 09/21/2021	66. hBarn - REKT Unaudited \$18,000,000 05/17/2021	89. Creas Finance - REKT Bramah Systems \$8,000,000 07/03/2022	112. Belt - REKT Hooch \$6,300,000 05/29/2021
21. Harmony Bridge - REKT N/A \$100,000,000 06/23/2022	44. Crypto.com - REKT Deelito \$31,700,000 01/18/2022	67. Curio - REKT N/A \$16,000,000 03/25/2024	90. Superfluid - REKT Peckshield \$8,700,000 02/08/2022	113. Audius - REKT Kudekz, OpenZeppelin \$6,000,000 07/23/2022
22. NEO Bridge - HTX - REKT N/A \$99,100,000 11/22/2023	45. Meerkat Finance - BSC - REKT Unaudited \$32,000,000 05/04/2021	68. Indexed Finance - REKT Unaudited \$16,000,000 01/18/2021	91. Platypus Finance - REKT Unaudited \$8,500,000 02/17/2023	114. Bodily - REKT Unaudited \$5,900,000 07/15/2021
23. Mirror Protocol - REKT Unaudited \$92,400,000 10/09/2021	46. Monet - REKT Nibarun, Peckshield \$31,000,000 11/30/2021	69. Team Finance - REKT Zokyo Security \$15,000,000 10/27/2022	92. Moola Market - REKT Aava \$8,400,000 10/19/2022	115. Inverse Finance - REKT 2 Unaudited \$5,800,000 04/16/2022

Figure: Top 115 most lucrative hacks over L2s. Data from rekt.news

Why do we need this Survey?



T&C | [leaderboard](#) | dark | en

1. Ronin Network - REKT Unaudited \$624,000,000 05/23/2022	24. Woofi - REKT Certik \$85,000,000 05/05/2024	47. Spartan Protocol - REKT N/A \$50,500,000 05/02/2021	70. Inverse Finance - REKT Unaudited \$15,000,000 04/02/2022	93. Visor Finance - REKT Unaudited \$8,200,000 12/21/2021
2. Poly Network - REKT Unaudited \$611,000,000 06/17/2021	25. Orbit Bridge - REKT Out of scope \$81,500,000 12/19/2023	48. Grim Finance - REKT Solidity Finance \$80,400,000 09/28/2021	71. Eminence - REkt in prod Unaudited \$15,000,000 09/28/2022	94. ThorChain - REKT ThorChain \$8,000,000 07/22/2021
3. BNB Bridge - REKT Unaudited \$598,000,000 10/08/2022	26. Fei Fari - REKT 2 Unaudited \$81,500,000 05/01/2022	49. Deribit - REKT N/A \$28,000,000 11/01/2022	72. Furucomo - REKT Unaudited \$14,000,000 02/27/2021	95. Hack Epidemic (Origi - REKT) Unaudited \$8,000,000 11/17/2022
4. BFB - MASK OFF N/A \$477,000,000 11/17/2022	27. Qubit Finance - REKT Unaudited \$80,000,000 01/28/2022	50. Wintermute - REKT N/A \$27,400,000 09/05/2022	73. Deus DAO - REKT 2 Arrow Labs \$13,400,000 04/28/2022	96. LCK - REKT Unaudited \$7,940,000 01/08/2022
5. Nornhale - REKT Readyset \$324,000,000 02/02/2022	28. Ascendex - REKT Unaudited \$77,700,000 12/12/2021	51. StableMagnet - REKT Tetherate \$27,400,000 04/23/2021	74. Compounder Finance - REKT out of scope \$12,000,000 12/29/2022	97. HTX (Huobi) - REKT N/A \$7,300,000 09/24/2022
6. Mixin Network - REKT N/A \$208,000,000 04/02/2023	29. Curve Vyper - REKT N/A \$80,000,000 07/08/2023	52. Paid Network - REKT Unaudited \$27,000,000 03/05/2021	75. Agave DAO - REKT Unaudited \$11,700,000 03/15/2022	98. Anyswap - REKT Unaudited \$7,900,000 07/10/2021
7. Euler Finance - REKT Sherlock \$197,000,000 03/13/2023	30. Munchables - REKT Entersoft \$42,500,000 03/26/2024	53. Kronos Finance - REKT N/A \$26,000,000 11/18/2023	76. PrimalFi - REKT PrimeFi \$11,000,000 03/28/2024	99. Narf Finance - REKT Hacken \$7,300,000 12/18/2022
8. BitMart - REKT N/A \$199,000,000 12/04/2021	31. AlphaPro - REKT N/A \$80,000,000 07/22/2023	54. Harvest Finance - REKT Hachhi, Peckshield \$25,000,000 10/26/2020	77. Yearn - REKT 2 Unaudited \$11,000,000 04/13/2023	100. Meter - REKT Unaudited \$7,700,000 02/06/2022
9. Nomad Bridge - REKT N/A \$199,000,000 08/07/2022	32. EasyFI - REKT Unaudited \$59,000,000 04/19/2021	55. Ankr & Helio - REKT N/A \$24,000,000 12/02/2022	78. Saddle Finance - REKT 2 Unaudited \$11,000,000 12/02/2021	101. Nightmare on Street N/A \$7,500,000 10/17/2022
10. Deustalk - REKT Unaudited \$181,000,000 04/17/2022	33. Uranium Finance - REKT Unaudited \$57,200,000 04/28/2021	56. Xtokens - REKT Peckshield \$24,000,000 05/12/2021	79. Value Defi - REKT 3 Unaudited \$11,000,000 05/07/2021	102. Jihuo's Protocol - REKT Unaudited \$7,300,000 05/18/2023
11. Wintermute - REKT N/A \$162,300,000 09/29/2022	34. bZx - REKT Unaudited \$55,000,000 01/05/2021	57. BALD Base - REKT N/A \$23,000,000 07/31/2023	80. Yearn - REKT Unaudited \$11,000,000 02/05/2021	103. Hundred Finance - REKT WhiteHabDAO \$7,400,000 04/15/2023
12. Compound - REKT Unaudited \$147,000,000 09/23/2021	35. CoinEx - REKT N/A \$55,000,000 09/12/2023	58. Elephant Money - REKT Solidity Finance \$22,200,000 04/12/2021	81. Degen Finance - REKT Peckshield \$10,000,000 02/18/2022	104. Exactly Protocol - REKT Out of scope \$7,200,000 08/18/2020
13. Vulcan Forged - REKT Unaudited \$148,000,000 12/13/2021	36. Kyber Finance - REKT ChainSecurity, Sherlock \$46,000,000 09/12/2023	59. Blizz Finance, Venn Protocol - REKT n/a \$21,000,000 05/12/2022	82. Arbitix Finance - REKT Certik \$10,000,000 01/04/2022	105. BurgerSwap - REKT Unaudited \$7,200,000 05/28/2021
14. Cross Finance - REKT 2 Unaudited \$130,000,000 10/27/2021	37. Cashio - REKT Unaudited \$48,000,000 03/23/2022	60. Transit Swap - REKT Out of scope \$21,200,000 10/02/2022	83. Rari Capital - REKT Timestamp \$10,000,000 05/08/2021	106. Value Defi - REKT Unaudited \$7,000,000 11/14/2022
15. Multichain - REKT N/A \$128,300,000 07/19/2023	38. PancakeBunny - REKT Unaudited \$45,000,000 05/19/2021	61. Unizen - REkt Heilborn, Verchaine \$21,000,000 05/08/2024	84. Value Defi - REKT 2 Unaudited \$10,000,000 05/05/2021	107. Abracadabra - REKT Unaudited \$6,300,000 01/30/2024
16. Polonex - REKT N/A \$126,000,000 11/17/2023	39. Kucoin - REKT Internal audit \$45,000,000 09/29/2026	62. Popscicle Finance - REKT Peckshield \$20,000,000 04/03/2021	85. Cover - REKT Arcadia Group \$9,400,000 12/29/2020	108. Dead DAD - REKT Unaudited \$6,340,000 05/05/2023
17. BondDAO - REKT Out of scope \$124,000,000 02/01/2023	40. Stake - REKT N/A \$41,600,000 09/04/2023	63. Pissicle Finance - REKT Unaudited \$19,700,000 11/22/2020	86. dyDX - REKT N/A \$10,000,000 11/18/2023	109. Lodestar Finance - REKT Unaudited \$6,300,000 12/10/2022
18. Badger - REKT Unaudited \$129,000,000 12/02/2021	41. Alpha Finance - REKT Quantstamp, Peckshield \$37,500,000 02/13/2021	64. Creas Finance - REKT Unaudited \$18,000,000 05/29/2021	87. Punk Protocol - REKT Unaudited \$6,500,000 06/17/2021	110. Alchemix - REKT Unaudited \$6,300,000 05/16/2021
19. Mango Markets - REKT Out of Scope \$115,000,000 10/01/2022	42. LastPass Users - REKT N/A \$37,000,000 12/14/2022	65. Snadog - REKT Unaudited \$18,100,000 11/25/2021	88. SafeMoon - REKT Unaudited \$6,500,000 05/23/2022	111. Seneca Protocol - REKT Halborn \$6,400,000 02/28/2024
20. Atomic Wallet - REKT Unaudited \$108,000,000 06/07/2023	43. Yee Finance - REKT Slowmist \$34,000,000 09/17/2021	66. bEarn - REKT Unaudited \$18,000,000 05/17/2021	89. Creas Finance - REKT Bramah Systems \$6,000,000 07/03/2022	112. Beli - REKT mascot \$6,300,000 05/29/2021
21. Harmony Bridge - REKT N/A \$100,000,000 06/23/2022	44. Crypto.com - REKT Deloitte \$33,700,000 01/18/2022	67. Curio - REKT N/A \$18,000,000 02/25/2024	90. SuperFluid - REKT Peckshield \$6,700,000 02/08/2022	113. Audius - REKT Kudelski, OpenZeppelin \$6,300,000 07/23/2022
22. HECO Bridge, HTX - REKT N/A \$99,100,000 11/22/2023	45. Meerkat Finance - BSC - REKT Unaudited \$32,000,000 05/04/2021	68. IndexFinance - REKT Unaudited \$16,000,000 01/14/2021	91. Platipus Finance - REKT Unaudited \$6,500,000 02/17/2023	114. Bodily - REKT Unaudited \$5,900,000 07/15/2021
23. Mirror Protocol - REKT Unaudited \$92,400,000 10/08/2021	46. Monet - REKT Web3n, Peckshield \$31,400,000 11/08/2021	69. Team Finance - REKT Zokyo Security \$15,000,000 10/27/2022	92. Moola Market - REKT N/A \$6,400,000 10/19/2022	115. Inverse Finance - REKT 2 Unaudited \$5,800,000 09/16/2022

Figure: 2023 hacks. Data from rekt.news

Why do we need this Survey?



T&C | [leaderboard](#) | dark | en

1. Ronin Network - REKT Unaudited \$624,000,000 03/23/2022	24. Woofi - REKT Certik \$85,000,000 05/05/2024	47. Spartan Protocol - REKT N/A \$50,500,000 05/02/2021	70. Inverse Finance - REKT Unaudited \$15,000,000 04/02/2022	93. Visor Finance - REKT Unaudited \$8,200,000 12/21/2021
2. Poly Network - REKT Unaudited \$611,000,000 06/17/2021	25. Orbit Bridge - REKT Out of scope \$81,500,000 12/19/2023	48. Grim Finance - REKT Solidity Finance \$80,400,000 07/18/2021	71. Eminence - REkt in prod Unaudited \$15,000,000 09/28/2022	94. ThorChain - REKT 2 ThorChain \$8,000,000 07/22/2021
3. BNB Bridge - REKT Unaudited \$598,000,000 10/08/2022	26. Fei Rari - REKT 2 Unaudited \$81,000,000 05/01/2022	49. Deribit - REKT N/A \$28,000,000 11/01/2022	72. Furicomb - REKT Unaudited \$14,000,000 02/27/2021	95. Hack Epidemic (Origi - REKT) Unaudited \$8,000,000 11/17/2022
4. BFB - MASK OFF N/A \$477,000,000 12/13/2022	27. Qubit Finance - REKT Unaudited \$10,000,000 01/28/2022	50. Wintermute - REKT N/A \$27,400,000 09/05/2022	73. Deus DAO - REKT 2 Amor Labs \$13,400,000 04/28/2022	96. LCK - REKT Unaudited \$7,940,000 01/08/2022
5. Morpheus - REKT Readyto \$324,000,000 02/21/2022	28. Ascendex - REKT Unaudited \$77,700,000 12/12/2021	51. StableMagnet - REKT Techrate \$27,400,000 04/23/2021	74. Compounder Finance - REKT out of scope \$12,000,000 12/28/2022	97. HTX (Huobi) - REKT N/A \$7,300,000 09/24/2022
6. Maxin Network - REKT N/A \$208,000,000 04/02/2023	29. Curve Vyper - REKT N/A \$84,000,000 07/08/2023	52. Paid Network - REKT Unaudited \$27,000,000 03/05/2021	75. Agave DAO - REKT Unaudited \$11,700,000 03/15/2022	98. Anyswap - REKT Unaudited \$7,900,000 07/10/2021
7. Euler Finance - REKT Sherlock \$197,000,000 03/13/2023	30. Munchables - REKT Enterosaf \$80,000,000 03/26/2024	53. Kronos Finance - REKT N/A \$26,000,000 11/18/2023	76. PrimalFi - REKT PrimalFi \$11,600,000 03/28/2024	99. Narf Finance - REKT Hacken \$7,800,000 12/18/2022
8. BitMart - REKT N/A \$199,000,000 12/04/2021	31. AlphaPro - REKT N/A \$84,000,000 07/22/2023	54. Harvest Finance - REKT Hachhi, Peckshield \$25,000,000 10/26/2020	77. Yearn - REKT 2 Unaudited \$11,400,000 04/13/2023	100. Meter - REKT Unaudited \$7,700,000 02/06/2022
9. Nomad Bridge - REKT N/A \$190,000,000 08/07/2022	32. EasyFI - REKT Unaudited \$19,000,000 04/19/2021	55. Ankr & Helio - REKT N/A \$24,000,000 12/02/2022	78. Saddle Finance - REKT 2 Unaudited \$11,000,000 12/02/2021	101. Nightmare on Street N/A \$7,500,000 10/17/2023
10. Deustalk - REKT Unaudited \$181,000,000 04/17/2022	33. Uranium Finance - REKT Unaudited \$57,200,000 04/28/2021	56. Xtokens - REKT Peckshield \$24,000,000 05/12/2021	79. Value Defi - REKT 3 Unaudited \$11,000,000 05/07/2021	102. Jihuo's Protocol - REKT Unaudited \$7,300,000 05/18/2023
11. Wintermute - REKT N/A \$162,300,000 09/29/2022	34. bZx - REKT Unaudited \$55,000,000 11/05/2021	57. BALD Base - REKT N/A \$23,000,000 07/31/2023	80. Yearn - REKT Unaudited \$11,000,000 02/05/2021	103. Hundred Finance - REKT 2 WhiteHabDAO \$7,400,000 04/15/2023
12. Compound - REKT Unaudited \$147,000,000 03/21/2021	35. CoinEx - REKT N/A \$54,300,000 09/12/2023	58. Elephant Money - REKT Solidity Finance \$22,200,000 04/12/2021	81. Dego Finance - REKT Peckshield \$10,000,000 02/18/2022	104. Exactly Protocol - REKT Out of scope \$7,200,000 08/18/2020
13. Vulcan Forge - REKT Unaudited \$140,000,000 12/13/2021	36. KyberSwap - REKT ChainSecurity, Sherlock \$48,000,000 01/12/2023	59. Blizz Finance, Venus Protocol - REKT n/a \$21,000,000 04/13/2022	82. Arbitis Finance - REKT N/A \$10,000,000 01/04/2022	105. BurgerSwap - REKT Unaudited \$7,200,000 05/28/2021
14. Cross Finance - REKT 2 Unaudited \$130,000,000 10/27/2021	37. Cashio - REKT Unaudited \$48,000,000 03/23/2022	60. Transit Swap - REKT Out of scope \$21,000,000 10/02/2022	83. Rari Capital - REKT Quantstamp \$10,000,000 05/08/2021	106. Value Defi - REKT Unaudited \$7,000,000 11/14/2022
15. Multichain - REKT N/A \$128,300,000 08/19/2023	38. PancakeBunny - REKT Unaudited \$45,000,000 05/19/2021	61. Unizen - REKT Heilborn, Veritain \$21,000,000 05/08/2024	84. ValueDefi - REKT 2 Unaudited \$10,000,000 05/05/2021	107. Abracadabra - REKT Unaudited \$6,300,000 01/30/2024
16. Polonex - REKT N/A \$126,000,000 11/19/2023	39. Kucosin - REKT Internal audit \$45,000,000 09/29/2026	62. Popscile Finance - REKT Peckshield \$20,400,000 04/03/2021	85. Cover - REKT Arcadia Group \$9,400,000 12/29/2020	108. Dead DAD - REKT Unaudited \$6,300,000 05/05/2022
17. BondDAO - REKT Out of scope \$124,000,000 02/01/2023	40. Stake - REKT N/A \$41,600,000 09/04/2023	63. Pissicle Finance - REKT Unaudited \$19,700,000 11/22/2020	86. dydx - REKT N/A \$9,000,000 11/18/2023	109. Lodestar Finance - REKT Unaudited \$6,300,000 12/10/2022
18. Badger - REKT Unaudited \$120,000,000 12/02/2021	41. Alpha Finance - REKT Quantstamp, Peckshield \$37,500,000 02/13/2021	64. Creas Finance - REKT Unaudited \$18,000,000 05/29/2021	87. Punk Protocol - REKT Unaudited \$8,500,000 06/17/2021	110. Alchemix - REKT Unaudited \$6,300,000 05/16/2021
19. Mango Markets - REKT Out of scope \$115,000,000 10/11/2022	42. LastPass Users - REKT N/A \$37,000,000 12/14/2022	65. Snodog - REKT Unaudited \$15,100,000 11/25/2021	88. Safeemo - REKT Unaudited \$8,100,000 05/23/2022	111. Seneca Protocol - REKT Halborn \$6,400,000 02/28/2024
20. Atomic Wallet - REKT Unaudited \$108,000,000 04/07/2023	43. Ven Finance - REKT Slowmist \$34,000,000 09/07/2021	66. bEarn - REKT Unaudited \$16,000,000 05/17/2021	89. Crema Finance - REKT Dramat Systems \$6,000,000 07/05/2022	112. Bell - REKT Hacchi \$6,300,000 05/29/2021
21. Harmony Bridge - REKT N/A \$100,000,000 08/23/2022	44. Crypto.to - REKT Deloitte \$33,700,000 01/07/2022	67. Curio - REKT N/A \$16,000,000 02/25/2024	90. Superfluid - REKT Peckshield \$6,700,000 02/08/2022	113. Audius - REKT KudeLoaki, OpenZeppelin \$6,300,000 07/23/2022
22. HECO Bridge - HTX - REKT N/A \$99,100,000 11/22/2023	45. Meerkat Finance - BSC - REKT Unaudited \$32,000,000 05/04/2021	68. Indexed Finance - REKT Unaudited \$16,000,000 01/14/2021	91. Platypus Finance - REKT Unaudited \$6,500,000 02/17/2023	114. Bodily - REKT Unaudited \$5,900,000 07/15/2021
23. Mirror Protocol - REKT Unaudited \$92,400,000 10/09/2021	46. Monet - REKT Walborn, Peckshield \$31,400,000 11/08/2021	69. Team Finance - REKT Zokyo Security \$15,000,000 10/27/2022	92. Moola Market - REKT N/A \$6,400,000 10/19/2022	115. Inverse Finance - REKT 2 Unaudited \$5,800,000 05/16/2022

Figure: 2023 and 2022 hacks. Data from rekt.news

Why do we need this Survey?



T&C | [leaderboard](#) | dark | en

1. Ronin Network - REKT Unaudited \$624,000,000 03/23/2022	24. Moofi - REKT Certik \$85,000,000 05/05/2024	47. Spartan Protocol - REKT N/A \$89,500,000 05/02/2021	70. Inverse Finance - REKT Unaudited \$15,600,000 04/02/2022	93. Visor Finance - REKT Unaudited \$8,200,000 12/21/2021
2. Poly Network - REKT Unaudited \$601,000,000 04/07/2023	25. Orbit Bridge - REKT Out of scope \$81,500,000 12/18/2023	48. Grim Finance - REKT Solidity Finance \$28,400,000 11/01/2022	71. Eminence - Rekt in prod Unaudited \$15,000,000 09/28/2022	94. THORChain - REKT 2 THORChain \$8,000,000 07/22/2021
3. BNB Bridge - REKT Unaudited \$598,000,000 10/08/2022	26. Fei Rari - REKT 2 Unaudited \$477,000,000 11/23/2022	49. Deribit - REKT N/A \$18,000,000 01/28/2022	72. Furucubo - REKT Unaudited \$14,000,000 02/27/2021	95. Hack Epidemic (Origi - REKT) Unaudited \$8,000,000 11/17/2022
4. SBF - MASK OFF N/A \$447,000,000 07/13/2022	27. Qubit Finance - REKT Unaudited \$18,000,000 01/28/2022	50. Wintermute - REKT N/A \$27,400,000 09/05/2022	73. Deus DAO - REKT 2 Arrow Labs \$13,400,000 04/28/2022	96. LCK - REKT Unaudited \$7,940,000 01/06/2022
5. Nornhale - REKT Headline \$304,400,000 02/07/2022	28. Ascendex - REKT Unaudited \$77,700,000 12/12/2021	51. StableMagnet - REKT Techrate \$27,400,000 04/23/2021	74. Compounder Finance - REKT out of scope \$12,000,000 12/02/2022	97. HTX (Huobi) - REKT N/A \$7,940,000 09/24/2022
6. Mixin Network - REKT N/A \$208,000,000 04/02/2023	29. Curve - REKT N/A \$30,200,000 07/20/2022	52. Paid Network - REKT Unaudited \$27,000,000 03/05/2021	75. Agave DAO - Numbered - REKT Unaudited \$11,700,000 03/15/2022	98. Anyswap - REKT Unaudited \$7,940,000 07/10/2021
7. Euler Finance - REKT Sherlock \$197,000,000 03/31/2023	30. Munchables - REKT Enterprisef \$81,500,000 03/26/2024	53. Kronos Finance - REKT N/A \$26,400,000 11/18/2023	76. PrimalFi - REKT PrimalFi \$11,600,000 03/26/2024	99. Narf Finance - REKT Hacken \$7,800,000 12/18/2022
8. BitMart - REKT N/A \$194,000,000 12/04/2021	31. AlphaPro - REKT N/A \$64,000,000 07/22/2023	54. Harvest Finance - REKT Hacchi, Peckshield \$26,400,000 10/26/2020	77. Yearn - REKT 2 Unaudited \$11,400,000 04/13/2023	100. Meter - REKT Unaudited \$7,740,000 02/06/2021
9. Homad Bridge - REKT N/A \$190,000,000 08/01/2022	32. EasyFI - REKT Unaudited \$19,000,000 04/19/2021	55. Ankr & Helio - REKT N/A \$24,000,000 12/02/2022	78. Saddle Finance - REKT 2 Unaudited \$11,000,000 12/02/2021	101. Nightmare on FTN Street N/A \$7,580,000 14/17/2022
10. Beannstalk - REKT Unaudited \$181,000,000 04/17/2022	33. Uranium Finance - REKT Unaudited \$57,200,000 04/28/2021	56. Xtokens - REKT Peckshield \$24,000,000 05/12/2021	79. Value Defi - REKT 3 Unaudited \$11,000,000 05/07/2021	102. Jihuo's Protocol - REKT Unaudited \$7,300,000 05/18/2023
11. Wintermute - REKT N/A \$162,300,000 09/29/2022	34. bZx - REKT Unaudited \$55,000,000 11/05/2021	57. BALD Base - REKT N/A \$23,000,000 07/31/2023	80. Yearn - REKT Unaudited \$11,000,000 02/05/2021	103. Hundred Finance - REKT WhiteHabDAO \$7,400,000 04/15/2023
12. Compound - REKT Unaudited \$147,000,000 04/23/2021	35. CoinEx - REKT N/A \$54,300,000 09/12/2023	58. Elephant Money - REKT Solidity Finance \$22,200,000 04/12/2021	81. Dego Finance - REKT Peckshield \$10,000,000 02/18/2022	104. Exactly Protocol - REKT Out of scope \$7,240,000 08/18/2020
13. Vulcan Forged - REKT Unaudited \$140,000,000 12/12/2021	36. KyberFinance - REKT ChainSecurity, Sherlock \$48,000,000 00/12/2023	59. Blizz Finance, Venn Protocol - REKT n/a \$21,000,000 05/12/2022	82. Arbitix Finance - REKT Certik \$10,000,000 01/04/2022	105. BurgerSwap - REKT Unaudited \$7,240,000 05/28/2021
14. Crass Finance - REKT 2 Unaudited \$130,000,000 10/27/2021	37. Cashio - REKT Unaudited \$48,000,000 05/23/2022	60. Transit Swap - REKT out of scope \$21,200,000 10/08/2022	83. Rari Capital - REKT Timestamp \$10,000,000 05/08/2021	106. Value Defi - REKT Unaudited \$7,000,000 11/14/2022
15. Multichain - REKT N/A \$128,300,000 08/17/2023	38. PancakeBunny - REKT Unaudited \$45,000,000 05/19/2021	61. Unizen - Rekt Holborn, Verdashain \$20,000,000 05/08/2024	84. Value DefI - REKT 2 Unaudited \$10,000,000 05/05/2021	107. Abracadabra - REKT Unaudited \$6,300,000 01/30/2024
16. Polonex - REKT N/A \$126,000,000 11/19/2023	39. Kucosin - REKT Internal audit \$45,000,000 09/29/2026	62. Popcycle Finance - REKT Peckshield \$20,400,000 04/03/2021	85. Cover - REKT Arcadia Group \$9,400,000 12/29/2020	108. DeFiDAO - REKT Unaudited \$6,300,000 05/05/2023
17. BondDAO - REKT Out of scope \$124,000,000 02/07/2023	40. Stake - REKT N/A \$41,600,000 09/04/2023	63. Pickle Finance - REKT Unaudited \$19,700,000 11/22/2020	86. dydx - REKT N/A \$9,000,000 11/18/2023	109. Lodestar Finance - REKT Unaudited \$6,300,000 12/10/2020
18. Badger - REKT Unaudited \$120,000,000 12/02/2021	41. Alpha Finance - REKT Quantstamp, Peckshield \$37,500,000 02/13/2021	64. Creas Finance - REKT Unaudited \$18,800,000 05/29/2021	87. Punk Protocol - REKT Unaudited \$8,950,000 06/17/2021	110. Alchemix - REKT Unaudited \$6,300,000 05/16/2021
19. Mango Markets - REKT Out of Scope \$115,000,000 10/11/2022	42. LastPass Users - REKT N/A \$37,000,000 12/14/2022	65. Snodog - REKT Unaudited \$8,100,000 11/25/2021	88. Safeemo - REKT Unaudited \$8,900,000 06/24/2022	111. Semocs Protocol - REKT Halborn \$6,400,000 02/28/2024
20. Atomic Wallet - REKT Unaudited \$108,000,000 06/07/2023	43. Yee Finance - REKT Slowmist \$34,000,000 09/17/2021	66. bEarn - REKT Unaudited \$7,200,000 05/17/2022	89. Cremas Finance - REKT Dramax Systems \$8,000,000 07/03/2022	112. Bell - REKT Marchi \$6,300,000 05/29/2021
21. Harmony Bridge - REKT N/A \$100,000,000 08/23/2022	44. Crypto.to - REKT Deloitte \$33,700,000 01/18/2022	67. Curio - REKT N/A \$7,000,000 02/25/2024	90. Superfluid - REKT Peckshield \$7,700,000 02/08/2022	113. Audius - REKT KudeLoeki, OpenZeppelin \$6,200,000 07/23/2022
22. HEDO Bridge - HTX - REKT N/A \$99,100,000 11/22/2023	45. Meerkat Finance - BSC - REKT Unaudited \$32,000,000 05/04/2021	68. Indexed Finance - REKT Unaudited \$7,000,000 10/14/2021	91. Platypus Finance - REKT Unaudited \$6,500,000 02/17/2023	114. Bodily - REKT Unaudited \$5,900,000 07/15/2021
23. Mirror Protocol - REKT Unaudited \$92,400,000 10/08/2021	46. Monet - REKT Walborn, Peckshield \$31,400,000 11/08/2021	69. Team Finance - REKT Zkory Security \$5,000,000 10/27/2022	92. Moola Market - REKT N/A \$6,400,000 10/19/2022	115. Inverse Finance - REKT 2 Unaudited \$5,800,000 09/16/2022

Figure: 2024, 2023 and 2022 hacks. Data from rekt.news

Table of Contents

- 1 Why does Layer 1 not scale?
 - Blockchain Trilemma
 - A little bit of history on reaching consensus
 - What does this have to do with blockchains?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
 - From Secure Cryptographic Primitives
 - From Reliable Consensus
 - From Reliable Consensus and Decentralisation
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

From Secure Cryptographic Primitives

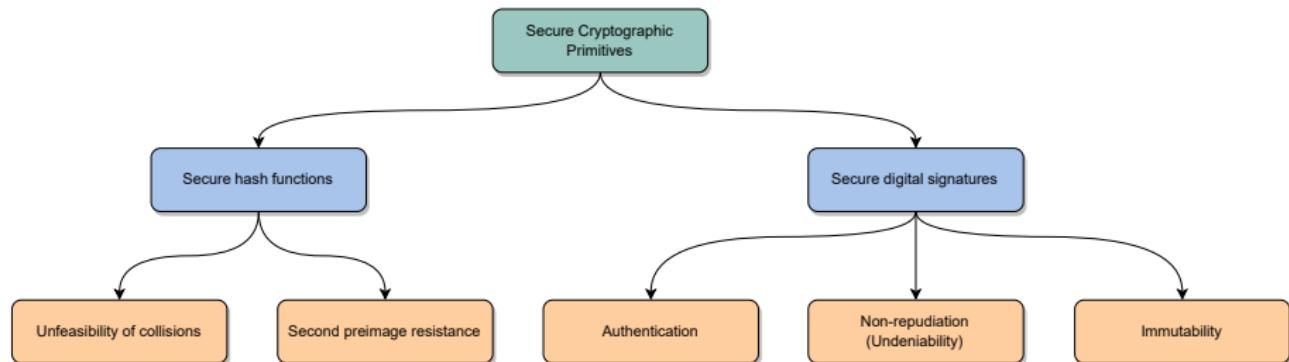


Figure: Security Assumptions derived from Secure Cryptographic Primitives.

From Reliable Consensus and Decentralisation

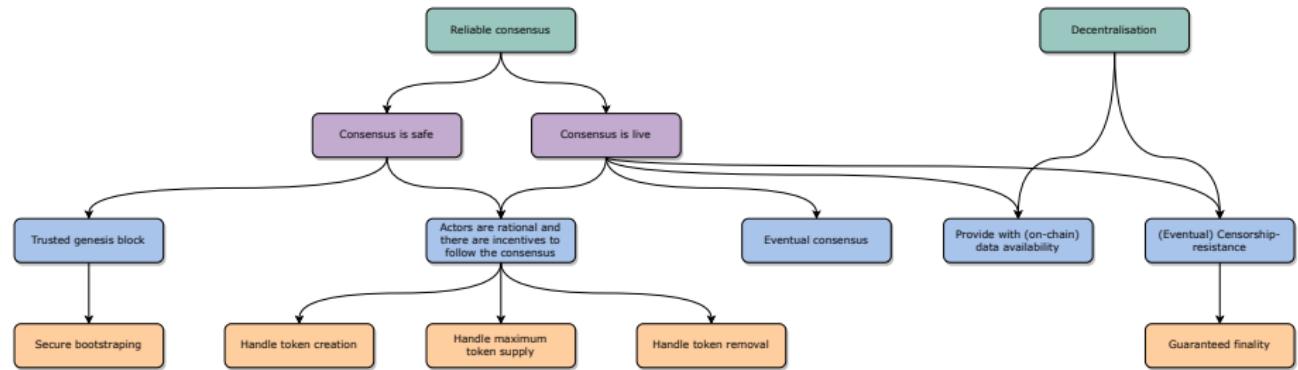


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

From Reliable Consensus

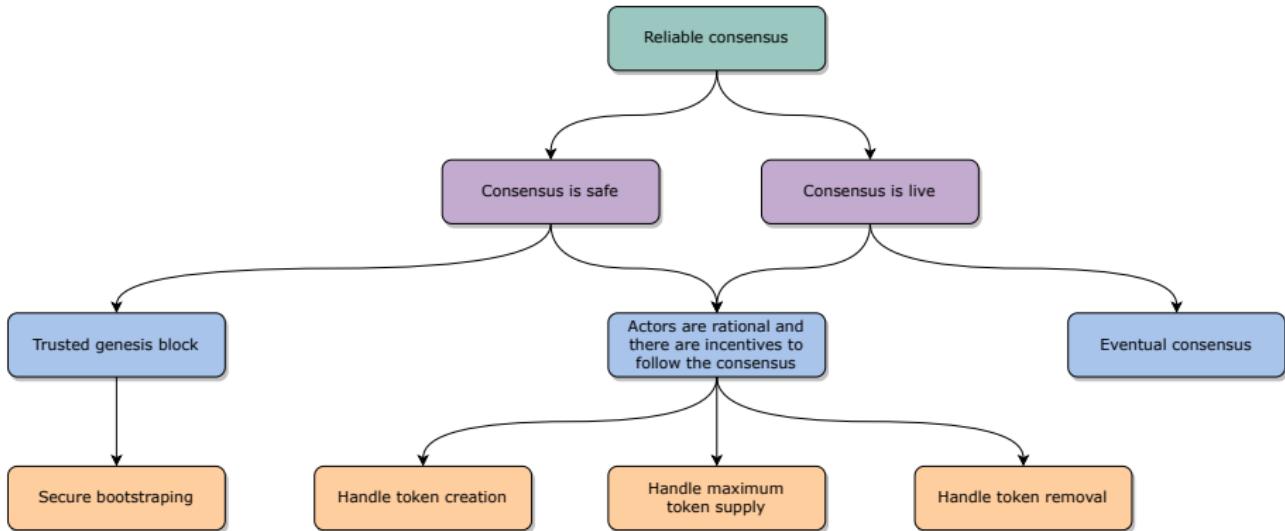


Figure: Security Assumptions derived from a Reliable Consensus.

From Reliable Consensus and Decentralisation

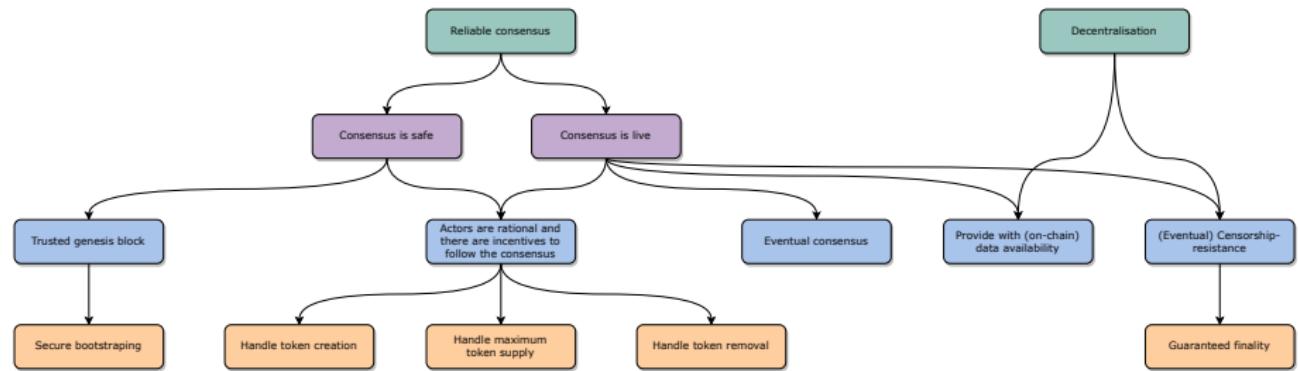


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

From Reliable Consensus and Decentralisation

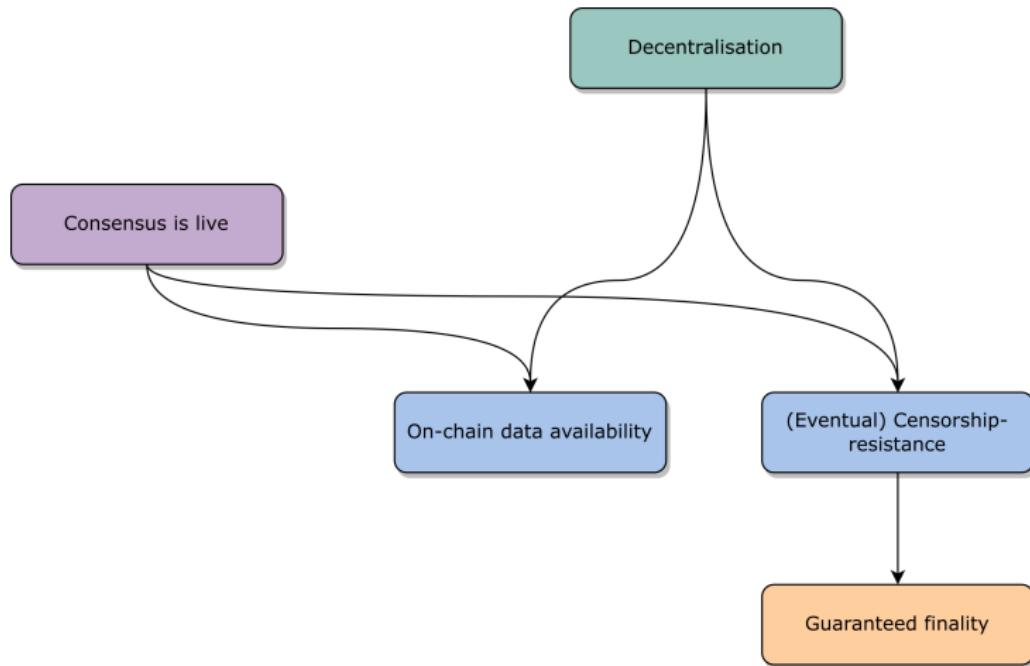


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

Table of Contents

- 1 Why does Layer 1 not scale?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Additional Security Assumptions for Layer 2

	Payment Channel Networks	Optimistic Rollups	Zero-Knowledge Rollups
Cryptographically secure hash functions (on L2 as well)	○	○	● ¹
Secure digital signatures (on L2 as well)	○	● ²	● ²
Consensus is safe and live	○	○	○
(Eventual) Censorship-resistance	○	○	○
Provide with on-chain data availability		○	○
Actors act rationally (on L2 as well)	○ ³	● ⁴	● ⁴
Bridge Smart Contract is Secure	●	●	●
Node is always online	●		
Fraud proofs have a wide enough time window		●	
Conversion from zkEVM to EVM is correctly done			●
Zero-Knowledge framework used is secure and sound			●
Trusted Setup is correctly generated (toxic waste safely disposed or generated using MPCs)			● ⁵

○ Inherited from layer 1.

● Inherited from layer 1, but modified.

● New additional security assumption.

¹ Zero-Knowledge Rollups may be using other "Zero-Knowledge Friendly" hash functions.

² Rollups may be using other signatures that enable them to aggregate several digital signatures together (e.g. BLS Signatures).

³ Actors on PCN need to act rationally when routing multi-hop payments, and when handling the closing of the channel.

⁴ Actors in Rollups need to act rationally and to have incentives to follow the rules.

⁵ Only for Zero-Knowledge Frameworks that require a Trusted Setup (usually SNARK-based).

Table of Contents

- 1 Why does Layer 1 not scale?
- 2 How do we scale blockchains?
- 3 Why do we need this study?
- 4 Security Assumptions for Layer 1
- 5 Additional Security Assumptions for Layer 2
- 6 Conclusions

Conclusions

- Security on Layer 2 is a concerning issue.

Conclusions

- Security on Layer 2 is a concerning issue.
- Every Layer 2 has additional security assumptions on top of Layer 1 security assumptions.

Conclusions

- Security on Layer 2 is a concerning issue.
- Every Layer 2 has additional security assumptions on top of Layer 1 security assumptions.
- Layer 2 is in constant evolution and (in some cases) not tested enough.

Conclusions

- Security on Layer 2 is a concerning issue.
- Every Layer 2 has additional security assumptions on top of Layer 1 security assumptions.
- Layer 2 is in constant evolution and (in some cases) not tested enough.
- Compromises between usability/convenience and additional security assumptions.

Conclusions

- Security on Layer 2 is a concerning issue.
- Every Layer 2 has additional security assumptions on top of Layer 1 security assumptions.
- Layer 2 is in constant evolution and (in some cases) not tested enough.
- Compromises between usability/convenience and additional security assumptions.
- Submitted to a Journal.

Thank you for your attention!



@0xAdriaTorralba



0xAdriaTorralba



atorralbaag@uoc.edu



QR Code to my research

