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

[1]Universitat Oberta de Catalunya
K-riptography and Information Security for Open Networks (KISON) Research Group

[2]Universitat Autònoma de Barcelona
SENDA - Security of Networks and Distributed Applications

[3]Cybercat - Center for Cybersecurity Research of Catalonia

April 19th, 2024

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Table of Contents

Table of Contents

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**

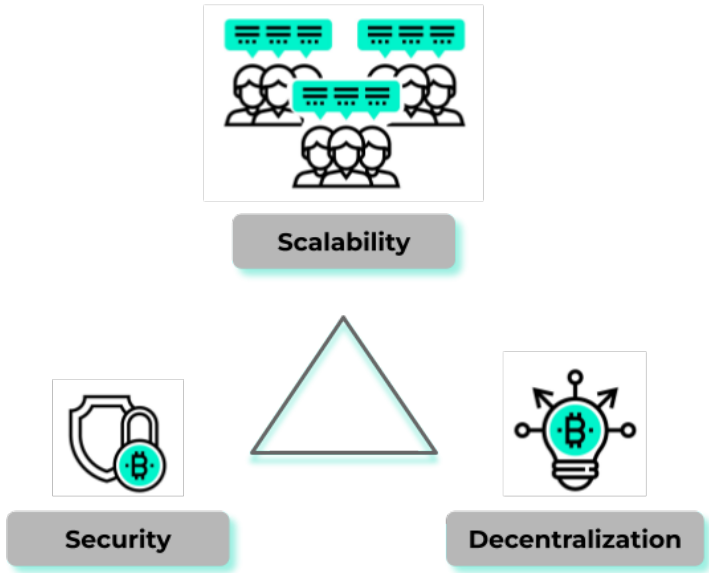


Figure: Diagram of the Blockchain Trilemma

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?

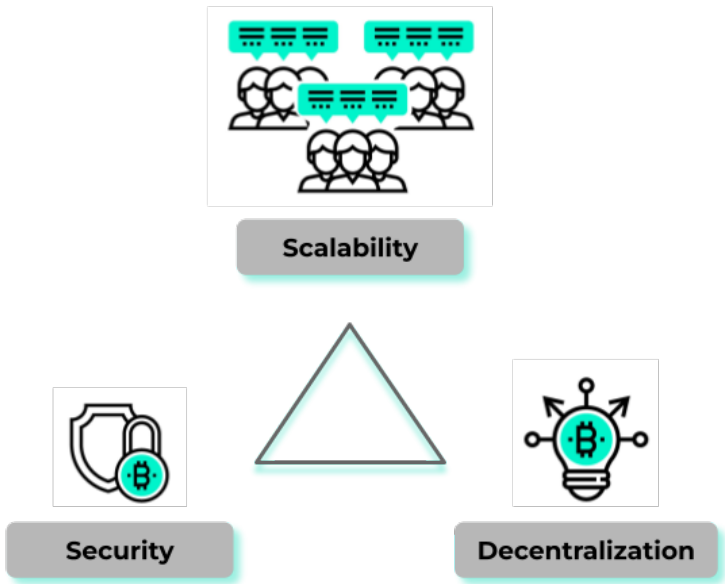
- The CAP theorem, under **Partition-tolerance**, announced a trade-off between,
  - **Consistency,**
  - **Availability.**
- It **might be possible** to relate

$$\text{CAP theorem} \iff \text{Blockchain trilemma}$$

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

$$\text{CAP theorem} \iff \text{Blockchain trilemma}$$



Thank you for your attention!

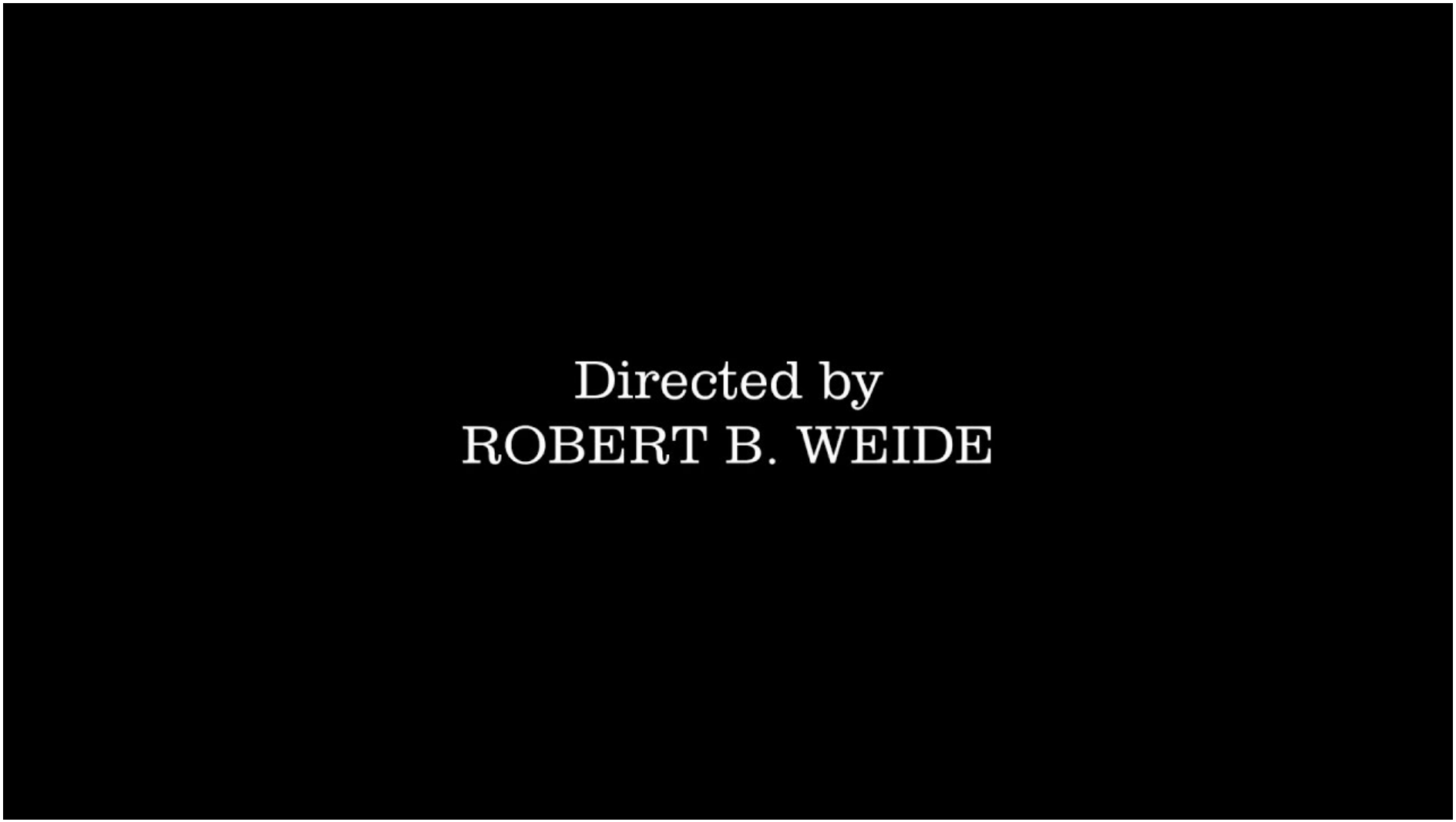
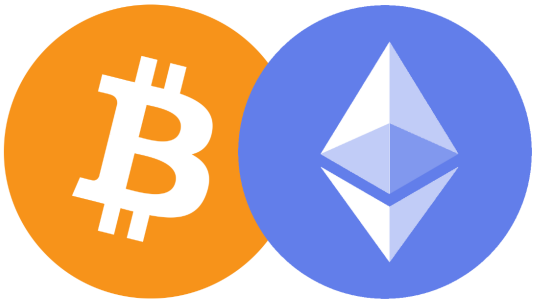
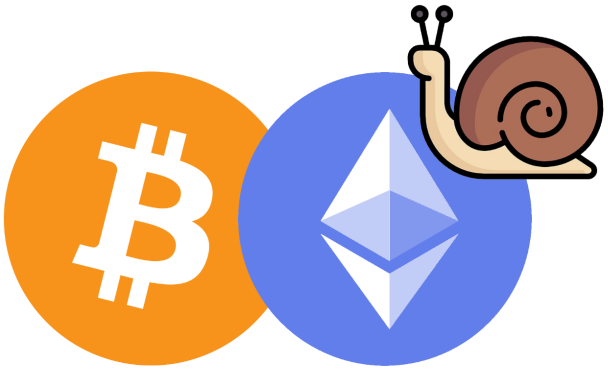


Table of Contents

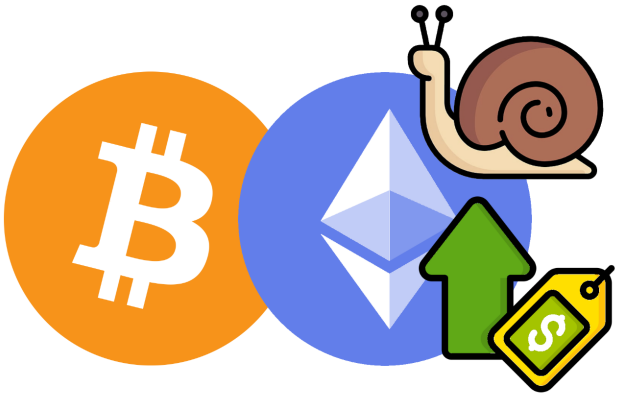
Bitcoin and Ethereum do not scale



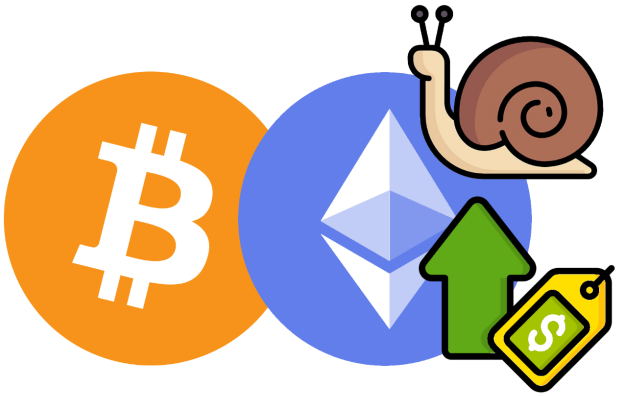
Slow

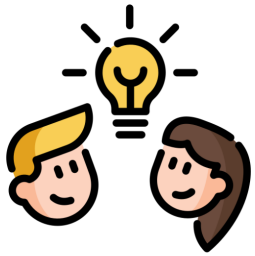


Expensive

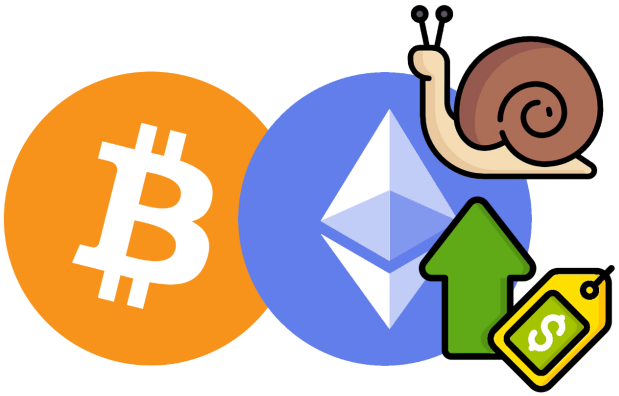


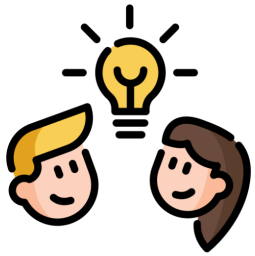
But people have ideas... Layer 2!

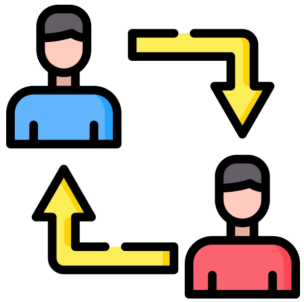




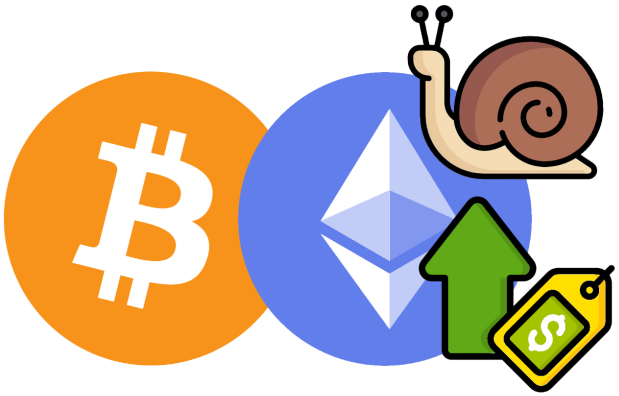
Payment Channel Networks

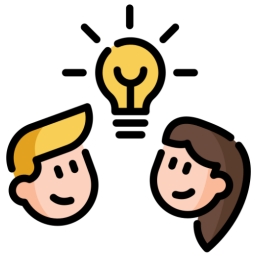


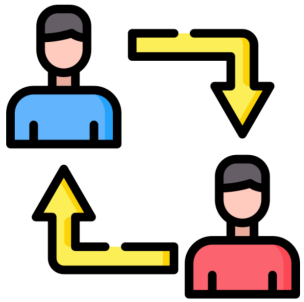


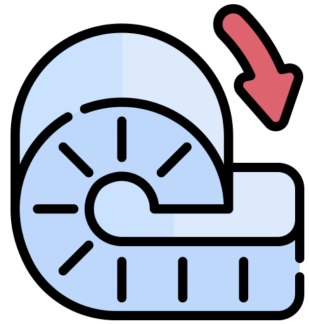


Zero-Knowledge Rollups and Optimistic Rollups

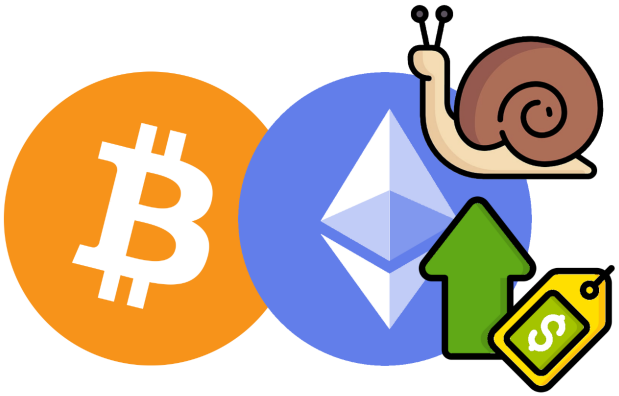


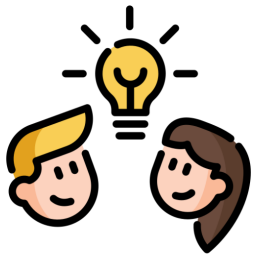


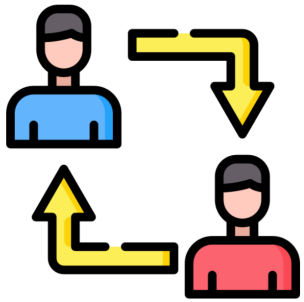


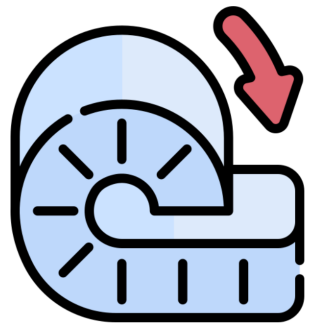


Bridges to enable interoperability

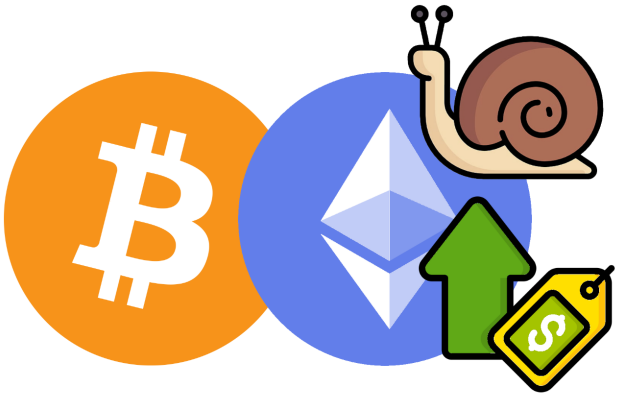


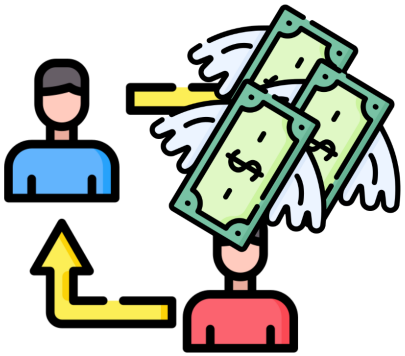


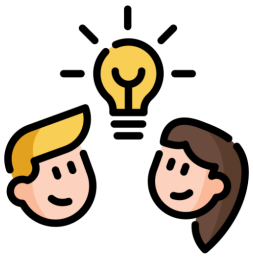


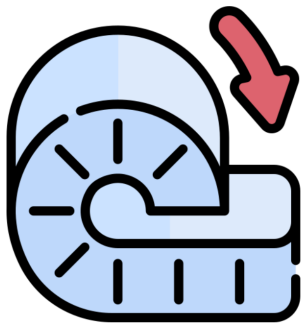


Money

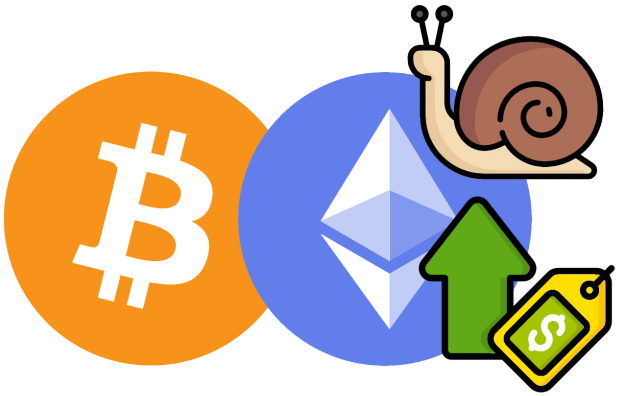


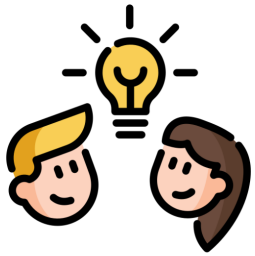


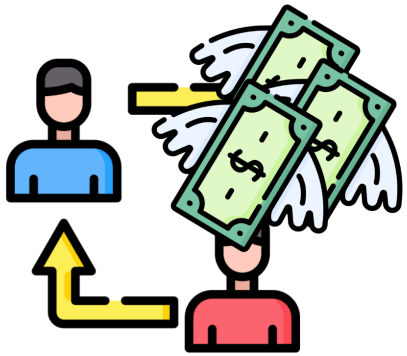


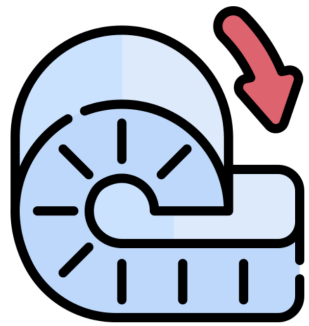


More money...

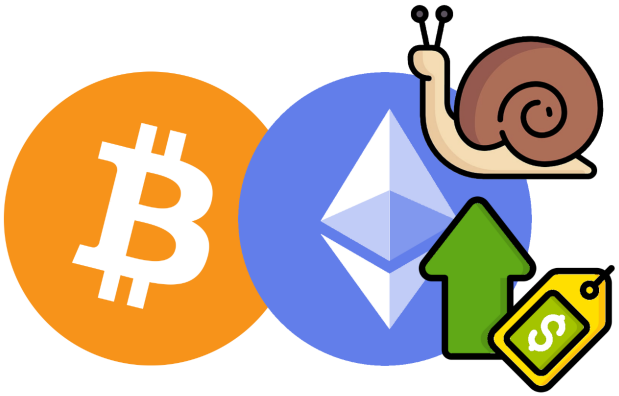


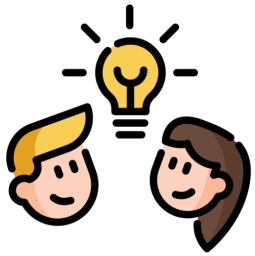


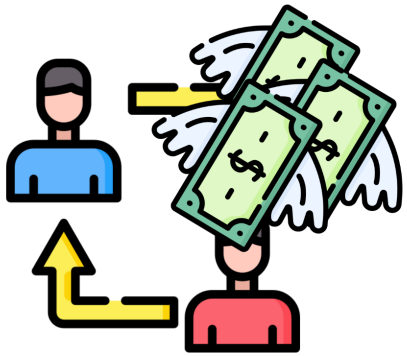


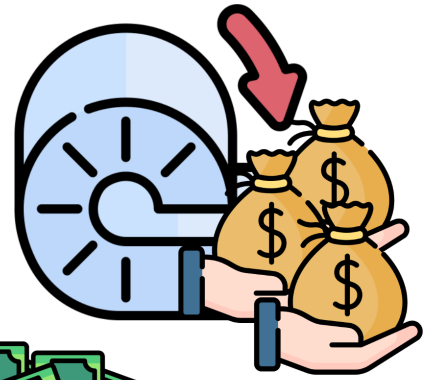


Even more money

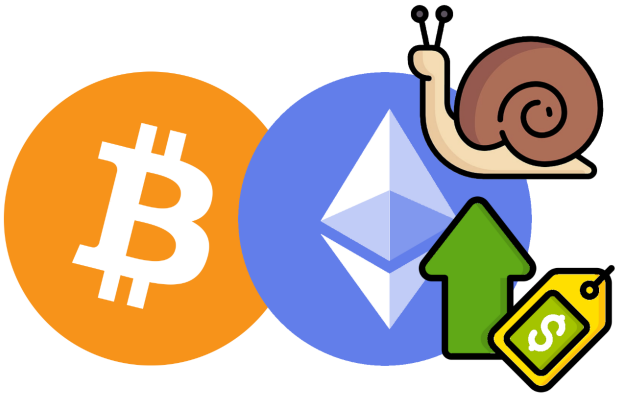


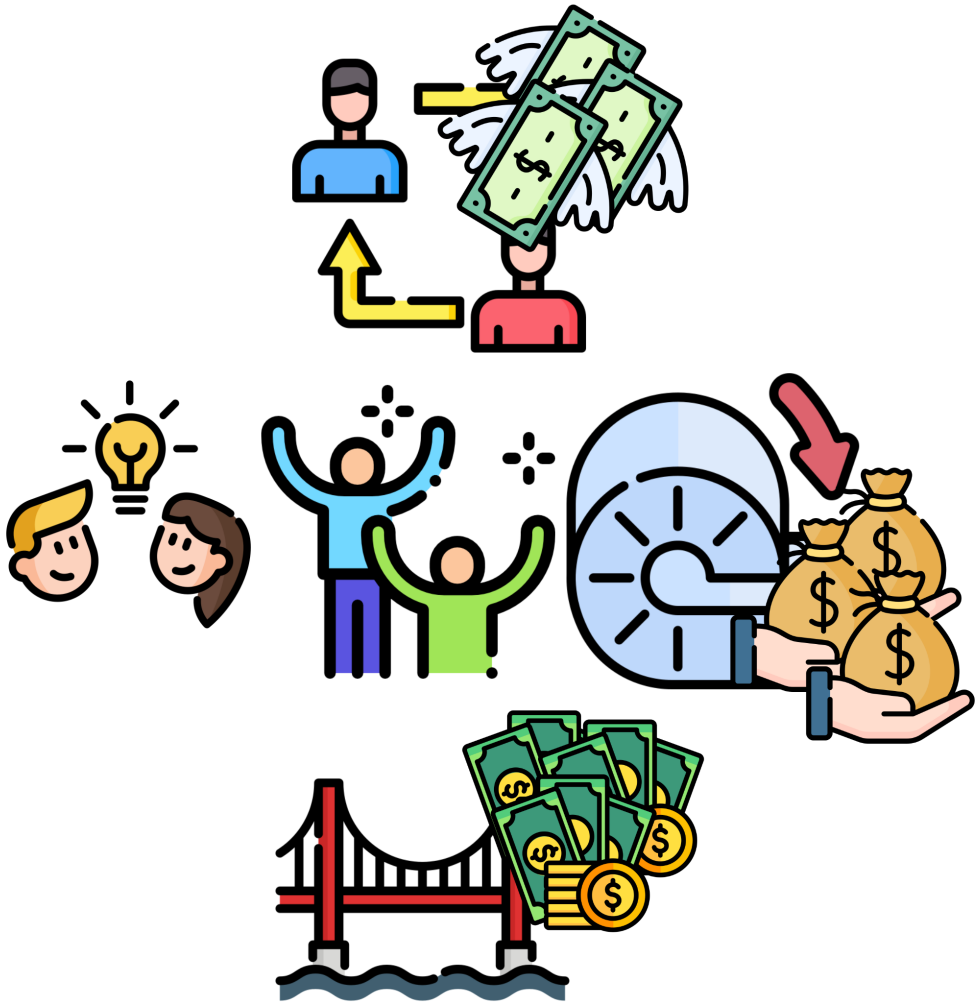




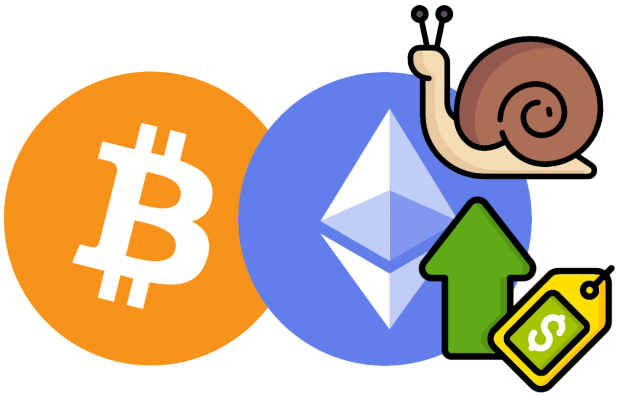


So... everybody is happy :)





So... everybody is happy :)



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

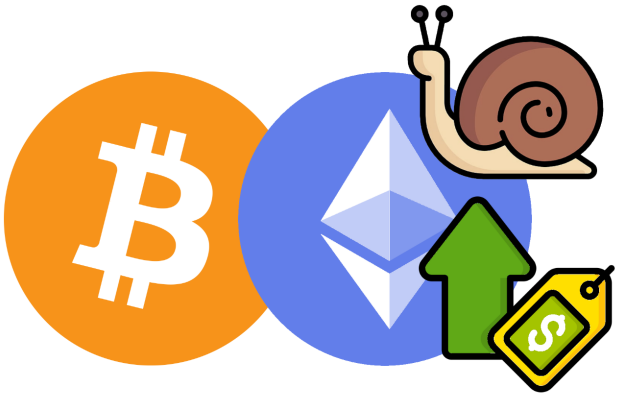


Table of Contents

Why do we need this Survey?

rekt

T&C | leaderboard | dark | en

1. **Ronin Network - REKT** *Unaudited*
   $624.000.000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611.000.000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586.000.000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477.000.000 | 11/12/2022
5. **Wormhole - REKT** *Neodyme*
   $326.000.000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
   $200.000.000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
   $197.000.000 | 03/13/2023
8. **BitMart - REKT** *N/A*
   $196.000.000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
   $190.000.000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
    $181.000.000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
    $162.300.000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
    $147.000.000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
    $140.000.000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
    $130.000.000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
    $126.300.000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
    $126.000.000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
    $120.000.000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
    $120.000.000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
    $115.000.000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
    $100.000.000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
    $100.000.000 | 06/23/2022
22. **HECO Bridge, HTX - REKT** *N/A*
    $99.100.000 | 11/22/2023
23. **Mirror Protocol - REKT** *Unaudited*
    $92.000.000 | 10/08/2021
24. **Woofi - Rekt** *Certik*
    $85.000.000 | 03/05/2024
25. **Orbit Bridge - REKT** *Out of scope*
    $81.500.000 | 12/31/2023
26. **Fei Rari - REKT 2** *Unaudited*
    $80.000.000 | 05/01/2022
27. **Qubit Finance - REKT** *Unaudited*
    $80.000.000 | 01/28/2022
28. **Ascendex - REKT** *Unaudited*
    $77.700.000 | 12/12/2021
29. **Curve, Vyper - REKT** *N/A*
    $69.300.000 | 07/30/2023
30. **Munchables - REKT** *Entersof*
    $62.500.000 | 03/26/2024
31. **AlphaPo - REKT** *N/A*
    $60.000.000 | 07/22/2023
32. **EasyFi - REKT** *Unaudited*
    $59.000.000 | 04/19/2021
33. **Uranium Finance - REKT** *Unaudited*
    $57.200.000 | 04/28/2021
34. **bZx - REKT** *Unaudited*
    $55.000.000 | 11/05/2021
35. **CoinEx - REKT** *N/A*
    $54.300.000 | 09/12/2023
36. **KyberSwap - REKT** *ChainSecurity, Sherlock*
    $48.000.000 | 11/22/2023
37. **Cashio - REKT** *Unaudited*
    $48.000.000 | 03/23/2022
38. **PancakeBunny - REKT** *Unaudited*
    $45.000.000 | 05/19/2021
39. **Kucoin - REKT** *Internal audit*
    $45.000.000 | 09/29/2020
40. **Stake - REKT** *N/A*
    $41.600.000 | 09/04/2023
41. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37.500.000 | 02/13/2021
42. **LastPass Users - REKT** *N/A*
    $37.000.000 | 12/14/2022
43. **Vee Finance - REKT** *Slowmist*
    $34.000.000 | 09/21/2021
44. **Crypto.com - REKT** *Deloitte*
    $33.700.000 | 01/18/2022
45. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32.000.000 | 03/04/2021
46. **MonoX - REKT** *Halborn, Peckshield*
    $31.400.000 | 11/30/2021
47. **Spartan Protocol - REKT** *N/A*
    $30.500.000 | 05/02/2021
48. **Grim Finance - REKT** *Solidity Finance*
    $30.000.000 | 12/18/2021
49. **Deribit - REKT** *N/A*
    $28.000.000 | 11/01/2022
50. **Wintermute - REKT** *N/A*
    $27.600.000 | 06/05/2022
51. **StableMagnet - REKT** *Techrate*
    $27.000.000 | 06/23/2021
52. **Paid Network - REKT** *Unaudited*
    $27.000.000 | 03/05/2021
53. **Kronos Research - REKT** *N/A*
    $26.000.000 | 11/18/2023
54. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25.000.000 | 10/26/2020
55. **Ankr & Helio - REKT** *N/A*
    $24.000.000 | 12/02/2022
56. **XToken - REKT** *Peckshield*
    $24.000.000 | 05/12/2021
57. **BALD on Base - REKT** *N/A*
    $23.000.000 | 07/31/2023
58. **Elephant Money - REKT** *Solidity Finance*
    $22.200.000 | 04/12/2021
59. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21.800.000 | 05/13/2022
60. **Transit Swap - REKT** *Out of scope*
    $21.200.000 | 10/02/2022
61. **Unizen - Rekt** *Halborn, Verichains*
    $21.000.000 | 03/08/2024
62. **Popsicle Finance - REKT** *Peckshield*
    $20.000.000 | 08/03/2021
63. **Pickle Finance - REKT** *Unaudited*
    $19.700.000 | 11/22/2020
64. **Cream Finance - REKT** *Unaudited*
    $18.800.000 | 08/30/2021
65. **Snowdog - REKT** *Unaudited*
    $18.100.000 | 11/25/2021
66. **bEarn - REKT** *Unaudited*
    $18.000.000 | 05/17/2021
67. **Curio - REKT** *N/A*
    $16.000.000 | 03/23/2024
68. **Indexed Finance - REKT** *Unaudited*
    $16.000.000 | 10/14/2021
69. **Team Finance - REKT** *Zokyo Security*
    $15.800.000 | 10/27/2022
70. **Inverse Finance - REKT** *Unaudited*
    $15.600.000 | 04/02/2022
71. **Eminence - Rekt in prod** *Unaudited*
    $15.000.000 | 09/28/2020
72. **Furucombo - REKT** *Unaudited*
    $14.000.000 | 02/27/2021
73. **Deus DAO - REKT 2** *Armor Labs*
    $13.400.000 | 04/28/2022
74. **Compounder Finance - REKT** *out of scope*
    $12.000.000 | 12/02/2020
75. **Agave DAO, Hundred - REKT** *Unaudited*
    $11.700.000 | 03/15/2022
76. **PrismaFi - REKT** *PrismaFi*
    $11.600.000 | 03/28/2024
77. **Yearn - REKT 2** *Unaudited*
    $11.400.000 | 04/13/2023
78. **Saddle Finance - REKT 2** *Unaudited*
    $11.000.000 | 12/02/2021
79. **Value DeFi - REKT 3** *Unaudited*
    $11.000.000 | 05/07/2021
80. **Yearn - REKT** *Unaudited*
    $11.000.000 | 02/05/2021
81. **Dego Finance - REKT** *Peckshield*
    $10.000.000 | 02/10/2022
82. **Arbix Finance - REKT** *Certik*
    $10.000.000 | 01/04/2022
83. **Rari Capital - REKT** *Quantstamp*
    $10.000.000 | 05/08/2021
84. **Value DeFi - REKT 2** *Unaudited*
    $10.000.000 | 05/05/2021
85. **Cover - REKT** *Arcadia Group*
    $9.400.000 | 12/29/2020
86. **dYdX - REKT** *N/A*
    $9.000.000 | 11/18/2023
87. **Punk Protocol - REKT** *Unaudited*
    $8.950.000 | 08/10/2021
88. **Safemoon - REKT** *Unaudited*
    $8.900.000 | 03/28/2023
89. **Crema Finance - REKT** *Bramah Systems*
    $8.800.000 | 07/02/2022
90. **Superfluid - REKT** *Peckshield*
    $8.700.000 | 02/08/2022
91. **Platypus Finance - REKT** *Unaudited*
    $8.500.000 | 02/17/2023
92. **Moola Market - REKT** *N/A*
    $8.400.000 | 10/19/2022
93. **Visor Finance - REKT** *Unaudited*
    $8.200.000 | 12/21/2021
94. **THORChain - REKT 2** *THORChain*
    $8.000.000 | 07/22/2021
95. **Hack Epidemic (Origi - REKT)** *Unaudited*
    $8.000.000 | 11/17/2020
96. **LCX - REKT** *Unaudited*
    $7.940.000 | 01/08/2022
97. **HTX (Huobi) - REKT** *N/A*
    $7.900.000 | 09/24/2023
98. **Anyswap - REKT** *Unaudited*
    $7.900.000 | 07/10/2021
99. **Warp Finance - REKT** *Hacken*
    $7.800.000 | 12/18/2020
100. **Meter - REKT** *Unaudited*
    $7.700.000 | 02/06/2022
101. **Nightmare on FTM Street** *N/A*
    $7.500.000 | 10/17/2023
102. **Jimbo's Protocol - REKT** *Unaudited*
    $7.500.000 | 05/28/2023
103. **Hundred Finance - REKT 2** *WhiteHatDAO*
    $7.400.000 | 04/15/2023
104. **Exactly Protocol - REKT** *Out of scope*
    $7.200.000 | 08/18/2023
105. **BurgerSwap - REKT** *Unaudited*
    $7.200.000 | 05/28/2021
106. **Value DeFi - REKT** *Unaudited*
    $7.000.000 | 11/14/2020
107. **Abracadabra - REKT** *Unaudited*
    $6.500.000 | 01/30/2024
108. **Deus DAO - R3KT** *Unaudited*
    $6.500.000 | 05/05/2023
109. **Lodestar Finance - REKT** *Unaudited*
    $6.500.000 | 12/10/2022
110. **Alchemix - REKT** *Unaudited*
    $6.500.000 | 06/16/2021
111. **Seneca Protocol - REKT** *Halborn*
    $6.400.000 | 02/28/2024
112. **Belt - REKT** *Haechi*
    $6.300.000 | 05/29/2021
113. **Audius - REKT** *Kudelski, OpenZeppelin*
    $6.000.000 | 07/23/2022
114. **Bondly - REKT** *Unaudited*
    $5.900.000 | 07/15/2021
115. **Inverse Finance - REKT 2** *Unaudited*
    $5.800.000 | 06/16/2022

Why do we need this Survey?

rekt

T&C | leaderboard | dark | en

1. **Ronin Network - REKT** *Unaudited*
   $624.000.000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611.000.000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586.000.000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477.000.000 | 11/12/2022
5. **Wormhole - REKT** *Neodyme*
   $326.000.000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
   $200.000.000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
   $197.000.000 | 03/13/2023
8. **BitMart - REKT** *N/A*
   $196.000.000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
   $190.000.000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
    $181.000.000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
    $162.300.000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
    $147.000.000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
    $140.000.000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
    $130.000.000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
    $126.300.000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
    $126.000.000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
    $120.000.000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
    $120.000.000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
    $115.000.000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
    $100.000.000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
    $100.000.000 | 06/23/2022
22. **HECO Bridge, HTX - REKT** *N/A*
    $99.100.000 | 11/22/2023
23. **Mirror Protocol - REKT** *Unaudited*
    $92.000.000 | 10/08/2021
24. **Woofi - Rekt** *Certik*
    $85.000.000 | 03/05/2024
25. **Orbit Bridge - REKT** *Out of scope*
    $81.500.000 | 12/31/2023
26. **Fei Rari - REKT 2** *Unaudited*
    $80.000.000 | 05/01/2022
27. **Qubit Finance - REKT** *Unaudited*
    $80.000.000 | 01/28/2022
28. **Ascendex - REKT** *Unaudited*
    $77.700.000 | 12/12/2021
29. **Curve, Vyper - REKT** *N/A*
    $69.300.000 | 07/30/2023
30. **Munchables - REKT** *Entersof*
    $62.500.000 | 03/26/2024
31. **AlphaPo - REKT** *N/A*
    $60.000.000 | 07/22/2023
32. **EasyFi - REKT** *Unaudited*
    $59.000.000 | 04/19/2021
33. **Uranium Finance - REKT** *Unaudited*
    $57.200.000 | 04/28/2021
34. **bZx - REKT** *Unaudited*
    $55.000.000 | 11/05/2021
35. **CoinEx - REKT** *N/A*
    $54.300.000 | 09/12/2023
36. **KyberSwap - REKT** *ChainSecurity, Sherlock*
    $48.000.000 | 11/22/2023
37. **Cashio - REKT** *Unaudited*
    $48.000.000 | 03/23/2022
38. **PancakeBunny - REKT** *Unaudited*
    $45.000.000 | 05/19/2021
39. **Kucoin - REKT** *Internal audit*
    $45.000.000 | 09/29/2020
40. **Stake - REKT** *N/A*
    $41.600.000 | 09/04/2023
41. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37.500.000 | 02/13/2021
42. **LastPass Users - REKT** *N/A*
    $37.000.000 | 12/14/2022
43. **Vee Finance - REKT** *Slowmist*
    $34.000.000 | 09/21/2021
44. **Crypto.com - REKT** *Deloitte*
    $33.700.000 | 01/18/2022
45. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32.000.000 | 03/04/2021
46. **MonoX - REKT** *Halborn, Peckshield*
    $31.400.000 | 11/30/2021
47. **Spartan Protocol - REKT** *N/A*
    $30.500.000 | 05/02/2021
48. **Grim Finance - REKT** *Solidity Finance*
    $30.000.000 | 12/18/2021
49. **Deribit - REKT** *N/A*
    $28.000.000 | 11/01/2022
50. **Wintermute - REKT** *N/A*
    $27.600.000 | 06/05/2022
51. **StableMagnet - REKT** *Techrate*
    $27.000.000 | 06/23/2021
52. **Paid Network - REKT** *Unaudited*
    $27.000.000 | 03/05/2021
53. **Kronos Research - REKT** *N/A*
    $26.000.000 | 11/18/2023
54. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25.000.000 | 10/26/2020
55. **Ankr & Helio - REKT** *N/A*
    $24.000.000 | 12/02/2022
56. **XToken - REKT** *Peckshield*
    $24.000.000 | 05/12/2021
57. **BALD on Base - REKT** *N/A*
    $23.000.000 | 07/31/2023
58. **Elephant Money - REKT** *Solidity Finance*
    $22.200.000 | 04/12/2021
59. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21.800.000 | 05/13/2022
60. **Transit Swap - REKT** *Out of scope*
    $21.200.000 | 10/02/2022
61. **Unizen - Rekt** *Halborn, Verichains*
    $21.000.000 | 03/08/2024
62. **Popsicle Finance - REKT** *Peckshield*
    $20.000.000 | 08/03/2021
63. **Pickle Finance - REKT** *Unaudited*
    $19.700.000 | 11/22/2020
64. **Cream Finance - REKT** *Unaudited*
    $18.800.000 | 08/30/2021
65. **Snowdog - REKT** *Unaudited*
    $18.100.000 | 11/25/2021
66. **bEarn - REKT** *Unaudited*
    $18.000.000 | 05/17/2021
67. **Curio - REKT** *N/A*
    $16.000.000 | 03/23/2024
68. **Indexed Finance - REKT** *Unaudited*
    $16.000.000 | 10/14/2021
69. **Team Finance - REKT** *Zokyo Security*
    $15.800.000 | 10/27/2022
70. **Inverse Finance - REKT** *Unaudited*
    $15.600.000 | 04/02/2022
71. **Eminence - Rekt in prod** *Unaudited*
    $15.000.000 | 09/28/2020
72. **Furucombo - REKT** *Unaudited*
    $14.000.000 | 02/27/2021
73. **Deus DAO - REKT 2** *Armor Labs*
    $13.400.000 | 04/28/2022
74. **Compounder Finance - REKT** *out of scope*
    $12.000.000 | 12/02/2020
75. **Agave DAO, Hundred - REKT** *Unaudited*
    $11.700.000 | 03/15/2022
76. **PrismaFi - REKT** *PrismaFi*
    $11.600.000 | 03/28/2024
77. **Yearn - REKT 2** *Unaudited*
    $11.400.000 | 04/13/2023
78. **Saddle Finance - REKT 2** *Unaudited*
    $11.000.000 | 12/02/2021
79. **Value DeFi - REKT 3** *Unaudited*
    $11.000.000 | 05/07/2021
80. **Yearn - REKT** *Unaudited*
    $11.000.000 | 02/05/2021
81. **Dego Finance - REKT** *Peckshield*
    $10.000.000 | 02/10/2022
82. **Arbix Finance - REKT** *Certik*
    $10.000.000 | 01/04/2022
83. **Rari Capital - REKT** *Quantstamp*
    $10.000.000 | 05/08/2021
84. **Value DeFi - REKT 2** *Unaudited*
    $10.000.000 | 05/05/2021
85. **Cover - REKT** *Arcadia Group*
    $9.400.000 | 12/29/2020
86. **dYdX - REKT** *N/A*
    $9.000.000 | 11/18/2023
87. **Punk Protocol - REKT** *Unaudited*
    $8.950.000 | 08/10/2021
88. **Safemoon - REKT** *Unaudited*
    $8.900.000 | 03/28/2023
89. **Crema Finance - REKT** *Bramah Systems*
    $8.800.000 | 07/02/2022
90. **Superfluid - REKT** *Peckshield*
    $8.700.000 | 02/08/2022
91. **Platypus Finance - REKT** *Unaudited*
    $8.500.000 | 02/17/2023
92. **Moola Market - REKT** *N/A*
    $8.400.000 | 10/19/2022
93. **Visor Finance - REKT** *Unaudited*
    $8.200.000 | 12/21/2021
94. **THORChain - REKT 2** *THORChain*
    $8.000.000 | 07/22/2021
95. **Hack Epidemic (Origi - REKT)** *Unaudited*
    $8.000.000 | 11/17/2020
96. **LCX - REKT** *Unaudited*
    $7.940.000 | 01/08/2022
97. **HTX (Huobi) - REKT** *N/A*
    $7.900.000 | 09/24/2023
98. **Anyswap - REKT** *Unaudited*
    $7.900.000 | 07/10/2021
99. **Warp Finance - REKT** *Hacken*
    $7.800.000 | 12/18/2020
100. **Meter - REKT** *Unaudited*
    $7.700.000 | 02/06/2022
101. **Nightmare on FTM Street** *N/A*
    $7.500.000 | 10/17/2023
102. **Jimbo's Protocol - REKT** *Unaudited*
    $7.500.000 | 05/28/2023
103. **Hundred Finance - REKT 2** *WhiteHatDAO*
    $7.400.000 | 04/15/2023
104. **Exactly Protocol - REKT** *Out of scope*
    $7.200.000 | 08/18/2023
105. **BurgerSwap - REKT** *Unaudited*
    $7.200.000 | 05/28/2021
106. **Value DeFi - REKT** *Unaudited*
    $7.000.000 | 11/14/2020
107. **Abracadabra - REKT** *Unaudited*
    $6.500.000 | 01/30/2024
108. **Deus DAO - R3KT** *Unaudited*
    $6.500.000 | 05/05/2023
109. **Lodestar Finance - REKT** *Unaudited*
    $6.500.000 | 12/10/2022
110. **Alchemix - REKT** *Unaudited*
    $6.500.000 | 06/16/2021
111. **Seneca Protocol - REKT** *Halborn*
    $6.400.000 | 02/28/2024
112. **Belt - REKT** *Haechi*
    $6.300.000 | 05/29/2021
113. **Audius - REKT** *Kudelski, OpenZeppelin*
    $6.000.000 | 07/23/2022
114. **Bondly - REKT** *Unaudited*
    $5.900.000 | 07/15/2021
115. **Inverse Finance - REKT 2** *Unaudited*
    $5.800.000 | 06/16/2022

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

Why do we need this Survey?

rekt

T&C | leaderboard | dark | en

1. **Ronin Network - REKT** *Unaudited*
   $624.000.000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611.000.000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586.000.000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477.000.000 | 11/12/2022
5. **Wormhole - REKT** *Neodyme*
   $326.000.000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
   $200.000.000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
   $197.000.000 | 03/13/2023
8. **BitMart - REKT** *N/A*
   $196.000.000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
   $190.000.000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
    $181.000.000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
    $162.300.000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
    $147.000.000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
    $140.000.000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
    $130.000.000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
    $126.300.000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
    $126.000.000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
    $120.000.000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
    $120.000.000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
    $115.000.000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
    $100.000.000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
    $100.000.000 | 06/23/2022
22. **HECO Bridge, HTX - REKT** *N/A*
    $99.100.000 | 11/22/2023
23. **Mirror Protocol - REKT** *Unaudited*
    $92.000.000 | 10/08/2021
24. **Woofi - Rekt** *Certik*
    $85.000.000 | 03/05/2024
25. **Orbit Bridge - REKT** *Out of scope*
    $81.500.000 | 12/31/2023
26. **Fei Rari - REKT 2** *Unaudited*
    $80.000.000 | 05/01/2022
27. **Qubit Finance - REKT** *Unaudited*
    $80.000.000 | 01/28/2022
28. **Ascendex - REKT** *Unaudited*
    $77.700.000 | 12/12/2021
29. **Curve, Vyper - REKT** *N/A*
    $69.300.000 | 07/30/2023
30. **Munchables - REKT** *Entersof*
    $62.500.000 | 03/26/2024
31. **AlphaPo - REKT** *N/A*
    $60.000.000 | 07/22/2023
32. **EasyFi - REKT** *Unaudited*
    $59.000.000 | 04/19/2021
33. **Uranium Finance - REKT** *Unaudited*
    $57.200.000 | 04/28/2021
34. **bZx - REKT** *Unaudited*
    $55.000.000 | 11/05/2021
35. **CoinEx - REKT** *N/A*
    $54.300.000 | 09/12/2023
36. **KyberSwap - REKT** *ChainSecurity, Sherlock*
    $48.000.000 | 11/22/2023
37. **Cashio - REKT** *Unaudited*
    $48.000.000 | 03/23/2022
38. **PancakeBunny - REKT** *Unaudited*
    $45.000.000 | 05/19/2021
39. **Kucoin - REKT** *Internal audit*
    $45.000.000 | 09/29/2020
40. **Stake - REKT** *N/A*
    $41.600.000 | 09/04/2023
41. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37.500.000 | 02/13/2021
42. **LastPass Users - REKT** *N/A*
    $37.000.000 | 12/14/2022
43. **Vee Finance - REKT** *Slowmist*
    $34.000.000 | 09/21/2021
44. **Crypto.com - REKT** *Deloitte*
    $33.700.000 | 01/18/2022
45. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32.000.000 | 03/04/2021
46. **MonoX - REKT** *Halborn, Peckshield*
    $31.400.000 | 11/30/2021
47. **Spartan Protocol - REKT** *N/A*
    $30.500.000 | 05/02/2021
48. **Grim Finance - REKT** *Solidity Finance*
    $30.000.000 | 12/18/2021
49. **Deribit - REKT** *N/A*
    $28.000.000 | 11/01/2022
50. **Wintermute - REKT** *N/A*
    $27.600.000 | 06/05/2022
51. **StableMagnet - REKT** *Techrate*
    $27.000.000 | 06/23/2021
52. **Paid Network - REKT** *Unaudited*
    $27.000.000 | 03/05/2021
53. **Kronos Research - REKT** *N/A*
    $26.000.000 | 11/18/2023
54. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25.000.000 | 10/26/2020
55. **Ankr & Helio - REKT** *N/A*
    $24.000.000 | 12/02/2022
56. **XToken - REKT** *Peckshield*
    $24.000.000 | 05/12/2021
57. **BALD on Base - REKT** *N/A*
    $23.000.000 | 07/31/2023
58. **Elephant Money - REKT** *Solidity Finance*
    $22.200.000 | 04/12/2021
59. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21.800.000 | 05/13/2022
60. **Transit Swap - REKT** *Out of scope*
    $21.200.000 | 10/02/2022
61. **Unizen - Rekt** *Halborn, Verichains*
    $21.000.000 | 03/08/2024
62. **Popsicle Finance - REKT** *Peckshield*
    $20.000.000 | 08/03/2021
63. **Pickle Finance - REKT** *Unaudited*
    $19.700.000 | 11/22/2020
64. **Cream Finance - REKT** *Unaudited*
    $18.800.000 | 08/30/2021
65. **Snowdog - REKT** *Unaudited*
    $18.100.000 | 11/25/2021
66. **bEarn - REKT** *Unaudited*
    $18.000.000 | 05/17/2021
67. **Curio - REKT** *N/A*
    $16.000.000 | 03/23/2024
68. **Indexed Finance - REKT** *Unaudited*
    $16.000.000 | 10/14/2021
69. **Team Finance - REKT** *Zokyo Security*
    $15.800.000 | 10/27/2022
70. **Inverse Finance - REKT** *Unaudited*
    $15.600.000 | 04/02/2022
71. **Eminence - Rekt in prod** *Unaudited*
    $15.000.000 | 09/28/2020
72. **Furucombo - REKT** *Unaudited*
    $14.000.000 | 02/27/2021
73. **Deus DAO - REKT 2** *Armor Labs*
    $13.400.000 | 04/28/2022
74. **Compounder Finance - REKT** *out of scope*
    $12.000.000 | 12/02/2020
75. **Agave DAO, Hundred - REKT** *Unaudited*
    $11.700.000 | 03/15/2022
76. **PrismaFi - REKT** *PrismaFi*
    $11.600.000 | 03/28/2024
77. **Yearn - REKT 2** *Unaudited*
    $11.400.000 | 04/13/2023
78. **Saddle Finance - REKT 2** *Unaudited*
    $11.000.000 | 12/02/2021
79. **Value DeFi - REKT 3** *Unaudited*
    $11.000.000 | 05/07/2021
80. **Yearn - REKT** *Unaudited*
    $11.000.000 | 02/05/2021
81. **Dego Finance - REKT** *Peckshield*
    $10.000.000 | 02/10/2022
82. **Arbix Finance - REKT** *Certik*
    $10.000.000 | 01/04/2022
83. **Rari Capital - REKT** *Quantstamp*
    $10.000.000 | 05/08/2021
84. **Value DeFi - REKT 2** *Unaudited*
    $10.000.000 | 05/05/2021
85. **Cover - REKT** *Arcadia Group*
    $9.400.000 | 12/29/2020
86. **dYdX - REKT** *N/A*
    $9.000.000 | 11/18/2023
87. **Punk Protocol - REKT** *Unaudited*
    $8.950.000 | 08/10/2021
88. **Safemoon - REKT** *Unaudited*
    $8.900.000 | 03/28/2023
89. **Crema Finance - REKT** *Bramah Systems*
    $8.800.000 | 07/02/2022
90. **Superfluid - REKT** *Peckshield*
    $8.700.000 | 02/08/2022
91. **Platypus Finance - REKT** *Unaudited*
    $8.500.000 | 02/17/2023
92. **Moola Market - REKT** *N/A*
    $8.400.000 | 10/19/2022
93. **Visor Finance - REKT** *Unaudited*
    $8.200.000 | 12/21/2021
94. **THORChain - REKT 2** *THORChain*
    $8.000.000 | 07/22/2021
95. **Hack Epidemic (Origi - REKT)** *Unaudited*
    $8.000.000 | 11/17/2020
96. **LCX - REKT** *Unaudited*
    $7.940.000 | 01/08/2022
97. **HTX (Huobi) - REKT** *N/A*
    $7.900.000 | 09/24/2023
98. **Anyswap - REKT** *Unaudited*
    $7.900.000 | 07/10/2021
99. **Warp Finance - REKT** *Hacken*
    $7.800.000 | 12/18/2020
100. **Meter - REKT** *Unaudited*
    $7.700.000 | 02/06/2022
101. **Nightmare on FTM Street** *N/A*
    $7.500.000 | 10/17/2023
102. **Jimbo's Protocol - REKT** *Unaudited*
    $7.500.000 | 05/28/2023
103. **Hundred Finance - REKT 2** *WhiteHatDAO*
    $7.400.000 | 04/15/2023
104. **Exactly Protocol - REKT** *Out of scope*
    $7.200.000 | 08/18/2023
105. **BurgerSwap - REKT** *Unaudited*
    $7.200.000 | 05/28/2021
106. **Value DeFi - REKT** *Unaudited*
    $7.000.000 | 11/14/2020
107. **Abracadabra - REKT** *Unaudited*
    $6.500.000 | 01/30/2024
108. **Deus DAO - R3KT** *Unaudited*
    $6.500.000 | 05/05/2023
109. **Lodestar Finance - REKT** *Unaudited*
    $6.500.000 | 12/10/2022
110. **Alchemix - REKT** *Unaudited*
    $6.500.000 | 06/16/2021
111. **Seneca Protocol - REKT** *Halborn*
    $6.400.000 | 02/28/2024
112. **Belt - REKT** *Haechi*
    $6.300.000 | 05/29/2021
113. **Audius - REKT** *Kudelski, OpenZeppelin*
    $6.000.000 | 07/23/2022
114. **Bondly - REKT** *Unaudited*
    $5.900.000 | 07/15/2021
115. **Inverse Finance - REKT 2** *Unaudited*
    $5.800.000 | 06/16/2022

Figure: 2023 hacks. Data from rekt.news

Why do we need this Survey?

rekt

T&C | leaderboard | dark | en

1. **Ronin Network - REKT** *Unaudited*
   $624.000.000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611.000.000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586.000.000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477.000.000 | 11/12/2022
5. **Wormhole - REKT** *Neodyme*
   $326.000.000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
   $200.000.000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
   $197.000.000 | 03/13/2023
8. **BitMart - REKT** *N/A*
   $196.000.000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
   $190.000.000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
    $181.000.000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
    $162.300.000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
    $147.000.000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
    $140.000.000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
    $130.000.000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
    $126.300.000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
    $126.000.000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
    $120.000.000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
    $120.000.000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
    $115.000.000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
    $100.000.000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
    $100.000.000 | 06/23/2022
22. **HECO Bridge, HTX - REKT** *N/A*
    $99.100.000 | 11/22/2023
23. **Mirror Protocol - REKT** *Unaudited*
    $92.000.000 | 10/08/2021
24. **Woofi - Rekt** *Certik*
    $85.000.000 | 03/05/2024
25. **Orbit Bridge - REKT** *Out of scope*
    $81.500.000 | 12/31/2023
26. **Fei Rari - REKT 2** *Unaudited*
    $80.000.000 | 05/01/2022
27. **Qubit Finance - REKT** *Unaudited*
    $80.000.000 | 01/28/2022
28. **Ascendex - REKT** *Unaudited*
    $77.700.000 | 12/12/2021
29. **Curve, Vyper - REKT** *N/A*
    $69.300.000 | 07/30/2023
30. **Munchables - REKT** *Entersof*
    $62.500.000 | 03/26/2024
31. **AlphaPo - REKT** *N/A*
    $60.000.000 | 07/22/2023
32. **EasyFi - REKT** *Unaudited*
    $59.000.000 | 04/19/2021
33. **Uranium Finance - REKT** *Unaudited*
    $57.200.000 | 04/28/2021
34. **bZx - REKT** *Unaudited*
    $55.000.000 | 11/05/2021
35. **CoinEx - REKT** *N/A*
    $54.300.000 | 09/12/2023
36. **KyberSwap - REKT** *ChainSecurity, Sherlock*
    $48.000.000 | 11/22/2023
37. **Cashio - REKT** *Unaudited*
    $48.000.000 | 03/23/2022
38. **PancakeBunny - REKT** *Unaudited*
    $45.000.000 | 05/19/2021
39. **Kucoin - REKT** *Internal audit*
    $45.000.000 | 09/29/2020
40. **Stake - REKT** *N/A*
    $41.600.000 | 09/04/2023
41. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37.500.000 | 02/13/2021
42. **LastPass Users - REKT** *N/A*
    $37.000.000 | 12/14/2022
43. **Vee Finance - REKT** *Slowmist*
    $34.000.000 | 09/21/2021
44. **Crypto.com - REKT** *Deloitte*
    $33.700.000 | 01/18/2022
45. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32.000.000 | 03/04/2021
46. **MonoX - REKT** *Halborn, Peckshield*
    $31.400.000 | 11/30/2021
47. **Spartan Protocol - REKT** *N/A*
    $30.500.000 | 05/02/2021
48. **Grim Finance - REKT** *Solidity Finance*
    $30.000.000 | 12/18/2021
49. **Deribit - REKT** *N/A*
    $28.000.000 | 11/01/2022
50. **Wintermute - REKT** *N/A*
    $27.600.000 | 06/05/2022
51. **StableMagnet - REKT** *Techrate*
    $27.000.000 | 06/23/2021
52. **Paid Network - REKT** *Unaudited*
    $27.000.000 | 03/05/2021
53. **Kronos Research - REKT** *N/A*
    $26.000.000 | 11/18/2023
54. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25.000.000 | 10/26/2020
55. **Ankr & Helio - REKT** *N/A*
    $24.000.000 | 12/02/2022
56. **XToken - REKT** *Peckshield*
    $24.000.000 | 05/12/2021
57. **BALD on Base - REKT** *N/A*
    $23.000.000 | 07/31/2023
58. **Elephant Money - REKT** *Solidity Finance*
    $22.200.000 | 04/12/2021
59. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21.800.000 | 05/13/2022
60. **Transit Swap - REKT** *Out of scope*
    $21.200.000 | 10/02/2022
61. **Unizen - Rekt** *Halborn, Verichains*
    $21.000.000 | 03/08/2024
62. **Popsicle Finance - REKT** *Peckshield*
    $20.000.000 | 08/03/2021
63. **Pickle Finance - REKT** *Unaudited*
    $19.700.000 | 11/22/2020
64. **Cream Finance - REKT** *Unaudited*
    $18.800.000 | 08/30/2021
65. **Snowdog - REKT** *Unaudited*
    $18.100.000 | 11/25/2021
66. **bEarn - REKT** *Unaudited*
    $18.000.000 | 05/17/2021
67. **Curio - REKT** *N/A*
    $16.000.000 | 03/23/2024
68. **Indexed Finance - REKT** *Unaudited*
    $16.000.000 | 10/14/2021
69. **Team Finance - REKT** *Zokyo Security*
    $15.800.000 | 10/27/2022
70. **Inverse Finance - REKT** *Unaudited*
    $15.600.000 | 04/02/2022
71. **Eminence - Rekt in prod** *Unaudited*
    $15.000.000 | 09/28/2020
72. **Furucombo - REKT** *Unaudited*
    $14.000.000 | 02/27/2021
73. **Deus DAO - REKT 2** *Armor Labs*
    $13.400.000 | 04/28/2022
74. **Compounder Finance - REKT** *out of scope*
    $12.000.000 | 12/02/2020
75. **Agave DAO, Hundred - REKT** *Unaudited*
    $11.700.000 | 03/15/2022
76. **PrismaFi - REKT** *PrismaFi*
    $11.600.000 | 03/28/2024
77. **Yearn - REKT 2** *Unaudited*
    $11.400.000 | 04/13/2023
78. **Saddle Finance - REKT 2** *Unaudited*
    $11.000.000 | 12/02/2021
79. **Value DeFi - REKT 3** *Unaudited*
    $11.000.000 | 05/07/2021
80. **Yearn - REKT** *Unaudited*
    $11.000.000 | 02/05/2021
81. **Dego Finance - REKT** *Peckshield*
    $10.000.000 | 02/10/2022
82. **Arbix Finance - REKT** *Certik*
    $10.000.000 | 01/04/2022
83. **Rari Capital - REKT** *Quantstamp*
    $10.000.000 | 05/08/2021
84. **Value DeFi - REKT 2** *Unaudited*
    $10.000.000 | 05/05/2021
85. **Cover - REKT** *Arcadia Group*
    $9.400.000 | 12/29/2020
86. **dYdX - REKT** *N/A*
    $9.000.000 | 11/18/2023
87. **Punk Protocol - REKT** *Unaudited*
    $8.950.000 | 08/10/2021
88. **Safemoon - REKT** *Unaudited*
    $8.900.000 | 03/28/2023
89. **Crema Finance - REKT** *Bramah Systems*
    $8.800.000 | 07/02/2022
90. **Superfluid - REKT** *Peckshield*
    $8.700.000 | 02/08/2022
91. **Platypus Finance - REKT** *Unaudited*
    $8.500.000 | 02/17/2023
92. **Moola Market - REKT** *N/A*
    $8.400.000 | 10/19/2022
93. **Visor Finance - REKT** *Unaudited*
    $8.200.000 | 12/21/2021
94. **THORChain - REKT 2** *THORChain*
    $8.000.000 | 07/22/2021
95. **Hack Epidemic (Origi - REKT)** *Unaudited*
    $8.000.000 | 11/17/2020
96. **LCX - REKT** *Unaudited*
    $7.940.000 | 01/08/2022
97. **HTX (Huobi) - REKT** *N/A*
    $7.900.000 | 09/24/2023
98. **Anyswap - REKT** *Unaudited*
    $7.900.000 | 07/10/2021
99. **Warp Finance - REKT** *Hacken*
    $7.800.000 | 12/18/2020
100. **Meter - REKT** *Unaudited*
    $7.700.000 | 02/06/2022
101. **Nightmare on FTM Street** *N/A*
    $7.500.000 | 10/17/2023
102. **Jimbo's Protocol - REKT** *Unaudited*
    $7.500.000 | 05/28/2023
103. **Hundred Finance - REKT 2** *WhiteHatDAO*
    $7.400.000 | 04/15/2023
104. **Exactly Protocol - REKT** *Out of scope*
    $7.200.000 | 08/18/2023
105. **BurgerSwap - REKT** *Unaudited*
    $7.200.000 | 05/28/2021
106. **Value DeFi - REKT** *Unaudited*
    $7.000.000 | 11/14/2020
107. **Abracadabra - REKT** *Unaudited*
    $6.500.000 | 01/30/2024
108. **Deus DAO - R3KT** *Unaudited*
    $6.500.000 | 05/05/2023
109. **Lodestar Finance - REKT** *Unaudited*
    $6.500.000 | 12/10/2022
110. **Alchemix - REKT** *Unaudited*
    $6.500.000 | 06/16/2021
111. **Seneca Protocol - REKT** *Halborn*
    $6.400.000 | 02/28/2024
112. **Belt - REKT** *Haechi*
    $6.300.000 | 05/29/2021
113. **Audius - REKT** *Kudelski, OpenZeppelin*
    $6.000.000 | 07/23/2022
114. **Bondly - REKT** *Unaudited*
    $5.900.000 | 07/15/2021
115. **Inverse Finance - REKT 2** *Unaudited*
    $5.800.000 | 06/16/2022

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

Why do we need this Survey?

rekt

T&C | leaderboard | dark | en

1. **Ronin Network - REKT** *Unaudited*
   $624.000.000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611.000.000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586.000.000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477.000.000 | 11/12/2022
5. **Wormhole - REKT** *Neodyme*
   $326.000.000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
   $200.000.000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
   $197.000.000 | 03/13/2023
8. **BitMart - REKT** *N/A*
   $196.000.000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
   $190.000.000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
    $181.000.000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
    $162.300.000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
    $147.000.000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
    $140.000.000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
    $130.000.000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
    $126.300.000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
    $126.000.000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
    $120.000.000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
    $120.000.000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
    $115.000.000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
    $100.000.000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
    $100.000.000 | 06/23/2022
22. **HECO Bridge, HTX - REKT** *N/A*
    $99.100.000 | 11/22/2023
23. **Mirror Protocol - REKT** *Unaudited*
    $92.000.000 | 10/08/2021
24. **Woofi - Rekt** *Certik*
    $85.000.000 | 03/05/2024
25. **Orbit Bridge - REKT** *Out of scope*
    $81.500.000 | 12/31/2023
26. **Fei Rari - REKT 2** *Unaudited*
    $80.000.000 | 05/01/2022
27. **Qubit Finance - REKT** *Unaudited*
    $80.000.000 | 01/28/2022
28. **Ascendex - REKT** *Unaudited*
    $77.700.000 | 12/12/2021
29. **Curve, Vyper - REKT** *N/A*
    $69.300.000 | 07/30/2023
30. **Munchables - REKT** *Entersof*
    $62.500.000 | 03/26/2024
31. **AlphaPo - REKT** *N/A*
    $60.000.000 | 07/22/2023
32. **EasyFi - REKT** *Unaudited*
    $59.000.000 | 04/19/2021
33. **Uranium Finance - REKT** *Unaudited*
    $57.200.000 | 04/28/2021
34. **bZx - REKT** *Unaudited*
    $55.000.000 | 11/05/2021
35. **CoinEx - REKT** *N/A*
    $54.300.000 | 09/12/2023
36. **KyberSwap - REKT** *ChainSecurity, Sherlock*
    $48.000.000 | 11/22/2023
37. **Cashio - REKT** *Unaudited*
    $48.000.000 | 03/23/2022
38. **PancakeBunny - REKT** *Unaudited*
    $45.000.000 | 05/19/2021
39. **Kucoin - REKT** *Internal audit*
    $45.000.000 | 09/29/2020
40. **Stake - REKT** *N/A*
    $41.600.000 | 09/04/2023
41. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37.500.000 | 02/13/2021
42. **LastPass Users - REKT** *N/A*
    $37.000.000 | 12/14/2022
43. **Vee Finance - REKT** *Slowmist*
    $34.000.000 | 09/21/2021
44. **Crypto.com - REKT** *Deloitte*
    $33.700.000 | 01/18/2022
45. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32.000.000 | 03/04/2021
46. **MonoX - REKT** *Halborn, Peckshield*
    $31.400.000 | 11/30/2021
47. **Spartan Protocol - REKT** *N/A*
    $30.500.000 | 05/02/2021
48. **Grim Finance - REKT** *Solidity Finance*
    $30.000.000 | 12/18/2021
49. **Deribit - REKT** *N/A*
    $28.000.000 | 11/01/2022
50. **Wintermute - REKT** *N/A*
    $27.600.000 | 06/05/2022
51. **StableMagnet - REKT** *Techrate*
    $27.000.000 | 06/23/2021
52. **Paid Network - REKT** *Unaudited*
    $27.000.000 | 03/05/2021
53. **Kronos Research - REKT** *N/A*
    $26.000.000 | 11/18/2023
54. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25.000.000 | 10/26/2020
55. **Ankr & Helio - REKT** *N/A*
    $24.000.000 | 12/02/2022
56. **XToken - REKT** *Peckshield*
    $24.000.000 | 05/12/2021
57. **BALD on Base - REKT** *N/A*
    $23.000.000 | 07/31/2023
58. **Elephant Money - REKT** *Solidity Finance*
    $22.200.000 | 04/12/2021
59. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21.800.000 | 05/13/2022
60. **Transit Swap - REKT** *Out of scope*
    $21.200.000 | 10/02/2022
61. **Unizen - Rekt** *Halborn, Verichains*
    $21.000.000 | 03/08/2024
62. **Popsicle Finance - REKT** *Peckshield*
    $20.000.000 | 08/03/2021
63. **Pickle Finance - REKT** *Unaudited*
    $19.700.000 | 11/22/2020
64. **Cream Finance - REKT** *Unaudited*
    $18.800.000 | 08/30/2021
65. **Snowdog - REKT** *Unaudited*
    $18.100.000 | 11/25/2021
66. **bEarn - REKT** *Unaudited*
    $18.000.000 | 05/17/2021
67. **Curio - REKT** *N/A*
    $16.000.000 | 03/23/2024
68. **Indexed Finance - REKT** *Unaudited*
    $16.000.000 | 10/14/2021
69. **Team Finance - REKT** *Zokyo Security*
    $15.800.000 | 10/27/2022
70. **Inverse Finance - REKT** *Unaudited*
    $15.600.000 | 04/02/2022
71. **Eminence - Rekt in prod** *Unaudited*
    $15.000.000 | 09/28/2020
72. **Furucombo - REKT** *Unaudited*
    $14.000.000 | 02/27/2021
73. **Deus DAO - REKT 2** *Armor Labs*
    $13.400.000 | 04/28/2022
74. **Compounder Finance - REKT** *out of scope*
    $12.000.000 | 12/02/2020
75. **Agave DAO, Hundred - REKT** *Unaudited*
    $11.700.000 | 03/15/2022
76. **PrismaFi - REKT** *PrismaFi*
    $11.600.000 | 03/28/2024
77. **Yearn - REKT 2** *Unaudited*
    $11.400.000 | 04/13/2023
78. **Saddle Finance - REKT 2** *Unaudited*
    $11.000.000 | 12/02/2021
79. **Value DeFi - REKT 3** *Unaudited*
    $11.000.000 | 05/07/2021
80. **Yearn - REKT** *Unaudited*
    $11.000.000 | 02/05/2021
81. **Dego Finance - REKT** *Peckshield*
    $10.000.000 | 02/10/2022
82. **Arbix Finance - REKT** *Certik*
    $10.000.000 | 01/04/2022
83. **Rari Capital - REKT** *Quantstamp*
    $10.000.000 | 05/08/2021
84. **Value DeFi - REKT 2** *Unaudited*
    $10.000.000 | 05/05/2021
85. **Cover - REKT** *Arcadia Group*
    $9.400.000 | 12/29/2020
86. **dYdX - REKT** *N/A*
    $9.000.000 | 11/18/2023
87. **Punk Protocol - REKT** *Unaudited*
    $8.950.000 | 08/10/2021
88. **Safemoon - REKT** *Unaudited*
    $8.900.000 | 03/28/2023
89. **Crema Finance - REKT** *Bramah Systems*
    $8.800.000 | 07/02/2022
90. **Superfluid - REKT** *Peckshield*
    $8.700.000 | 02/08/2022
91. **Platypus Finance - REKT** *Unaudited*
    $8.500.000 | 02/17/2023
92. **Moola Market - REKT** *N/A*
    $8.400.000 | 10/19/2022
93. **Visor Finance - REKT** *Unaudited*
    $8.200.000 | 12/21/2021
94. **THORChain - REKT 2** *THORChain*
    $8.000.000 | 07/22/2021
95. **Hack Epidemic (Origi - REKT)** *Unaudited*
    $8.000.000 | 11/17/2020
96. **LCX - REKT** *Unaudited*
    $7.940.000 | 01/08/2022
97. **HTX (Huobi) - REKT** *N/A*
    $7.900.000 | 09/24/2023
98. **Anyswap - REKT** *Unaudited*
    $7.900.000 | 07/10/2021
99. **Warp Finance - REKT** *Hacken*
    $7.800.000 | 12/18/2020
100. **Meter - REKT** *Unaudited*
    $7.700.000 | 02/06/2022
101. **Nightmare on FTM Street** *N/A*
    $7.500.000 | 10/17/2023
102. **Jimbo's Protocol - REKT** *Unaudited*
    $7.500.000 | 05/28/2023
103. **Hundred Finance - REKT 2** *WhiteHatDAO*
    $7.400.000 | 04/15/2023
104. **Exactly Protocol - REKT** *Out of scope*
    $7.200.000 | 08/18/2023
105. **BurgerSwap - REKT** *Unaudited*
    $7.200.000 | 05/28/2021
106. **Value DeFi - REKT** *Unaudited*
    $7.000.000 | 11/14/2020
107. **Abracadabra - REKT** *Unaudited*
    $6.500.000 | 01/30/2024
108. **Deus DAO - R3KT** *Unaudited*
    $6.500.000 | 05/05/2023
109. **Lodestar Finance - REKT** *Unaudited*
    $6.500.000 | 12/10/2022
110. **Alchemix - REKT** *Unaudited*
    $6.500.000 | 06/16/2021
111. **Seneca Protocol - REKT** *Halborn*
    $6.400.000 | 02/28/2024
112. **Belt - REKT** *Haechi*
    $6.300.000 | 05/29/2021
113. **Audius - REKT** *Kudelski, OpenZeppelin*
    $6.000.000 | 07/23/2022
114. **Bondly - REKT** *Unaudited*
    $5.900.000 | 07/15/2021
115. **Inverse Finance - REKT 2** *Unaudited*
    $5.800.000 | 06/16/2022

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

Table of Contents

From Secure Cryptographic Primitives

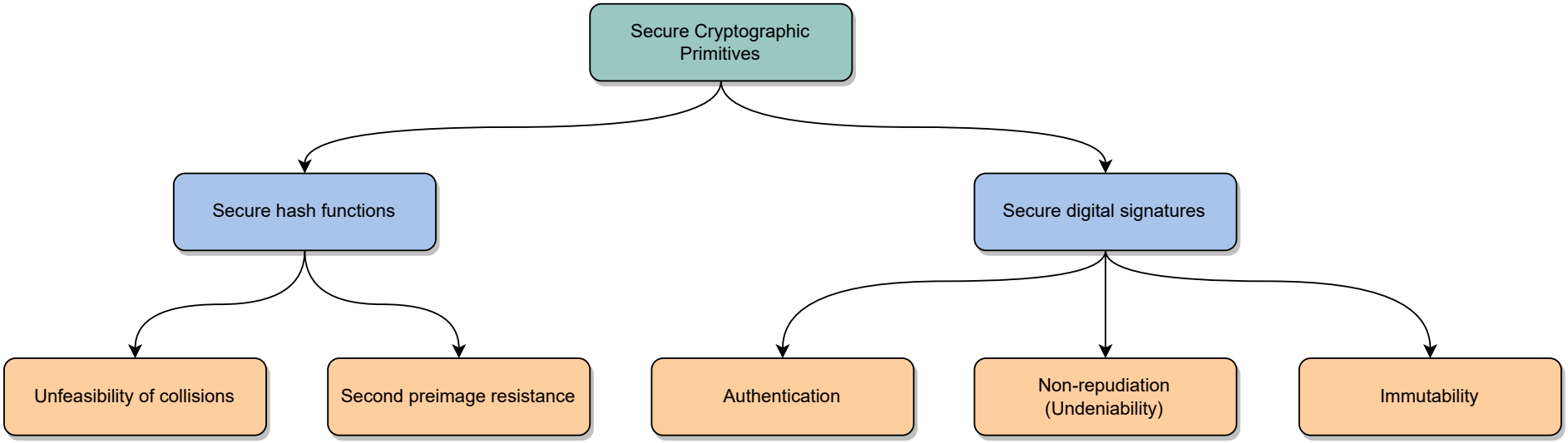


Figure: Security Assumptions derived from Secure Cryptographic Primitives.

From Reliable Consensus and Decentralisation

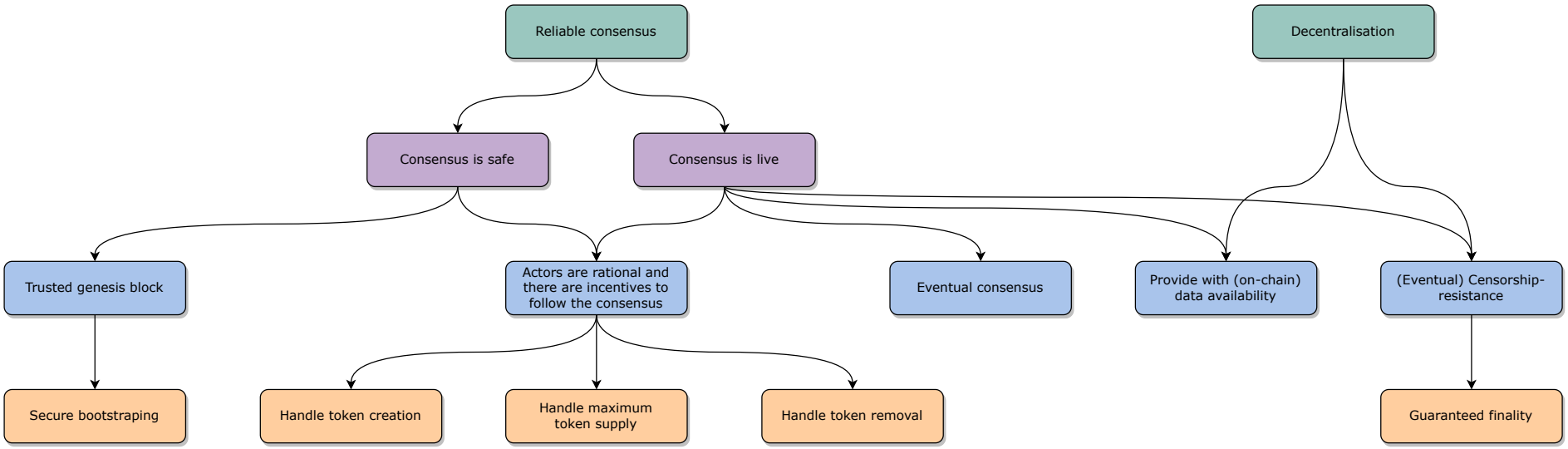


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

From Reliable Consensus

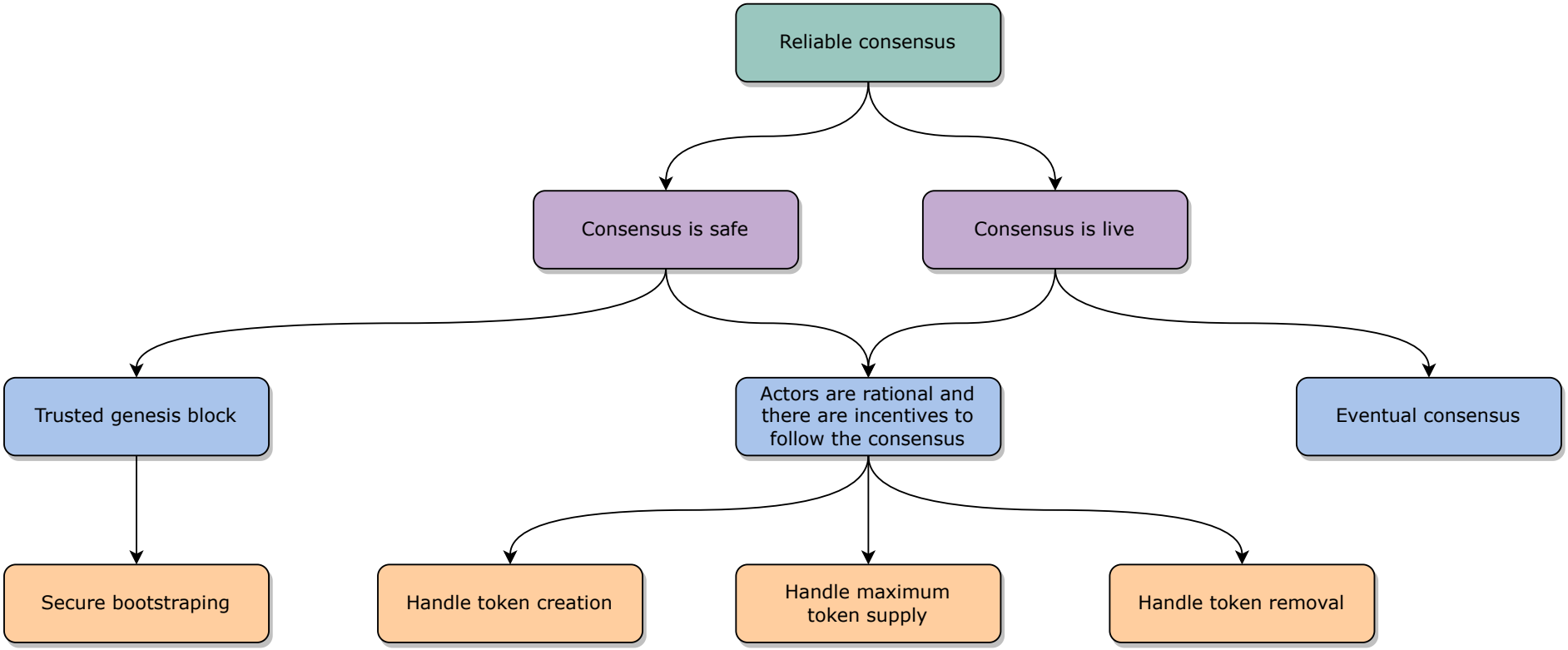


Figure: Security Assumptions derived from a Reliable Consensus.

From Reliable Consensus and Decentralisation

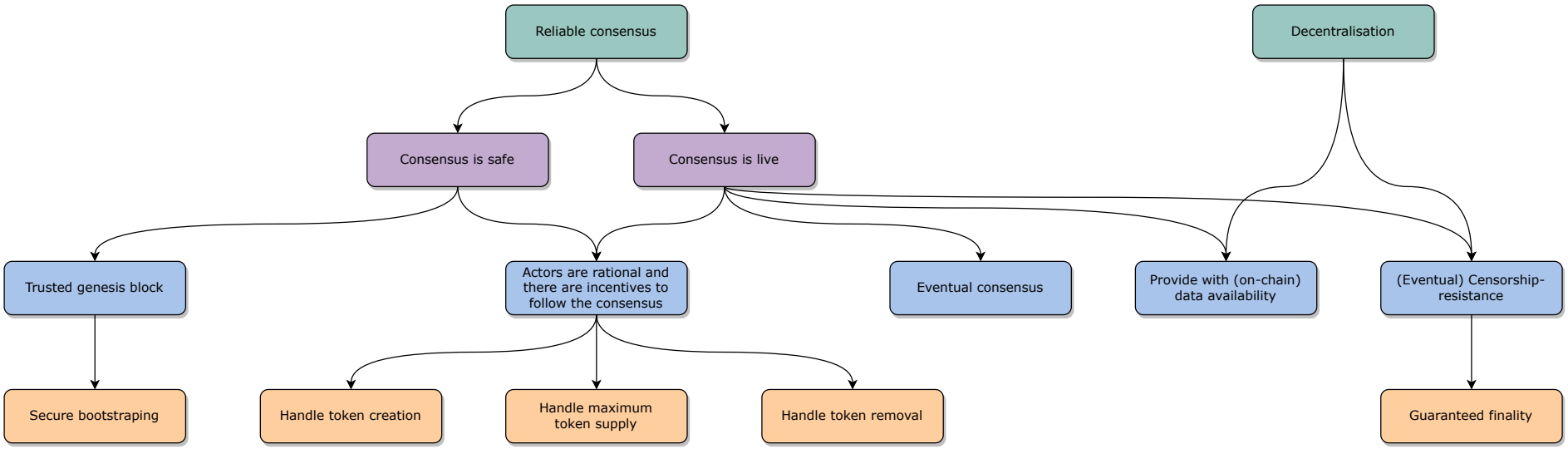


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

From Reliable Consensus and Decentralisation

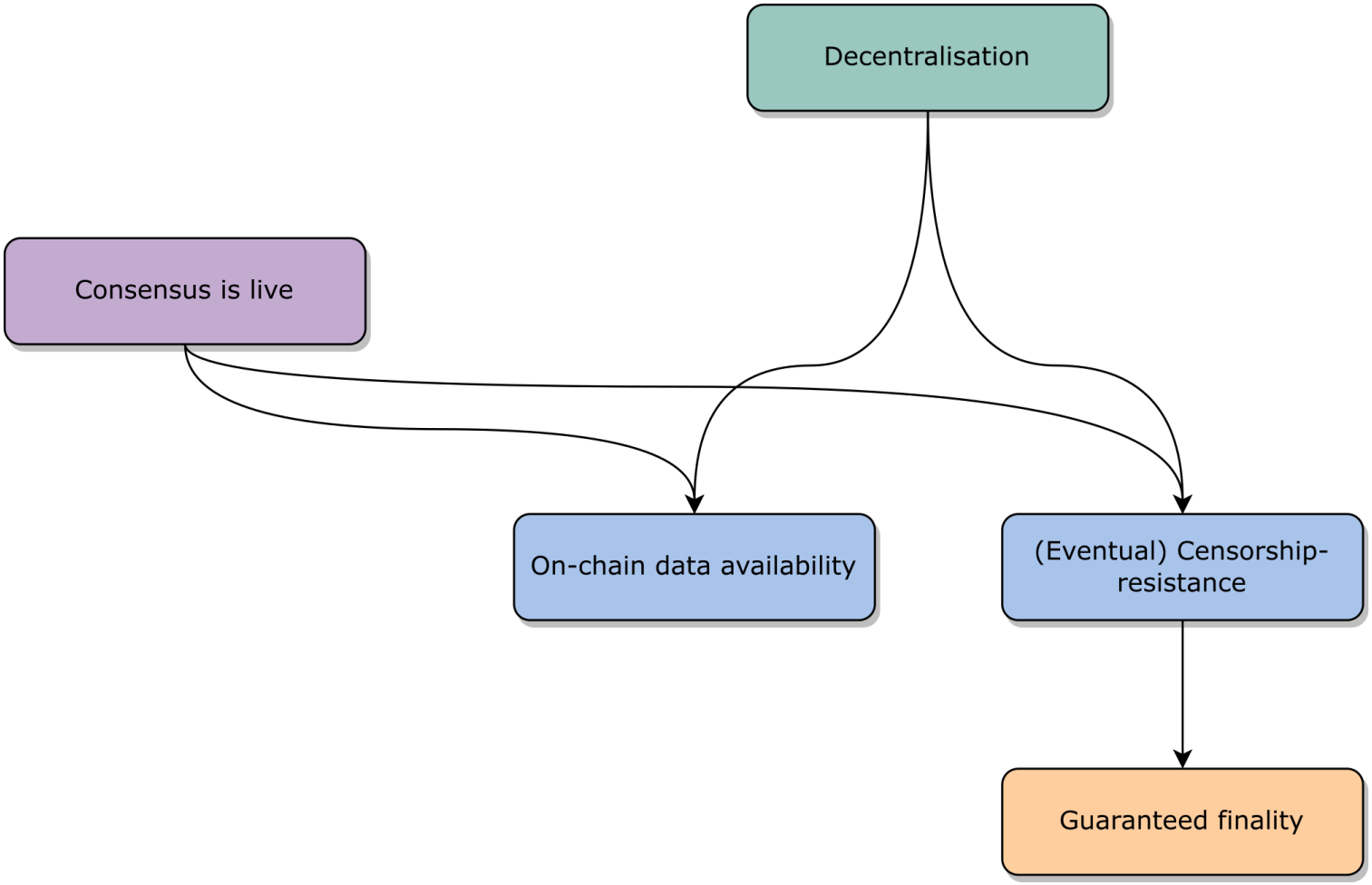


Figure: Security Assumptions derived from a Reliable Consensus and Decentralisation.

Table of Contents

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

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