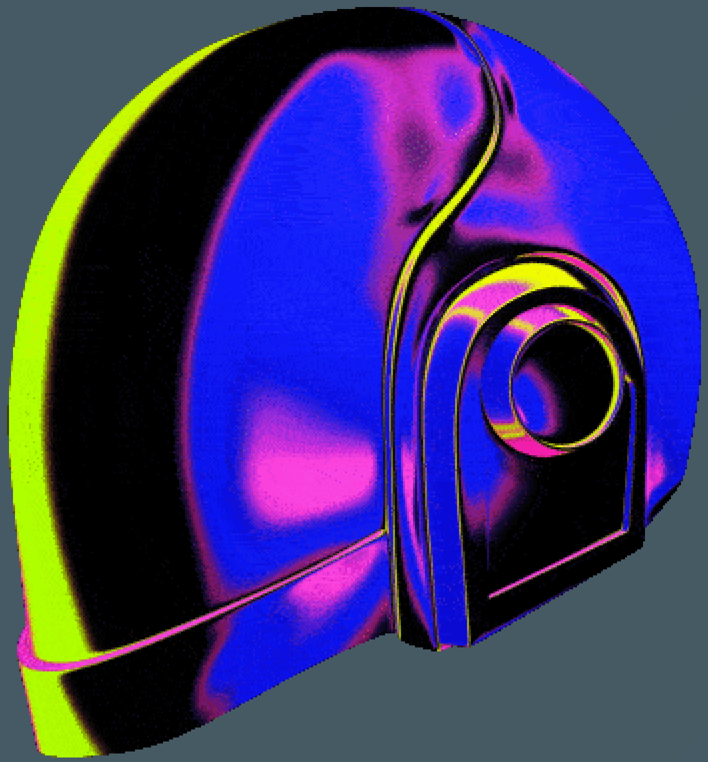


a CYPHERPUNK hackathon entry

Trust Graph for NPM

Enhancing Supply Chain Security with Community Trust

Our Team

Zb Tenerowicz	Leo Merinen	Chris Hiller

Our Goal

Create a distributed network of trust for sharing and consuming opinions on npm packages and their vulnerabilities.

- bootstrapped on the existing ecosystem
- possible to use "by the way" and trivial to adopt
- eliminate the need for an institution to take responsibility for the content

Trust Graph Explained

- Social graph of trust built on npm
- Users publish `@username/i_trust` packages
- Trust spreads proportionally through dependencies
- Simple and resistant to Sybil attacks

Trust Scores

- Derived from the user's position in the trust graph
- Range from 0 to 1
- Used to weigh assertions in the network
- Enables personalized, community-driven vulnerability assessments

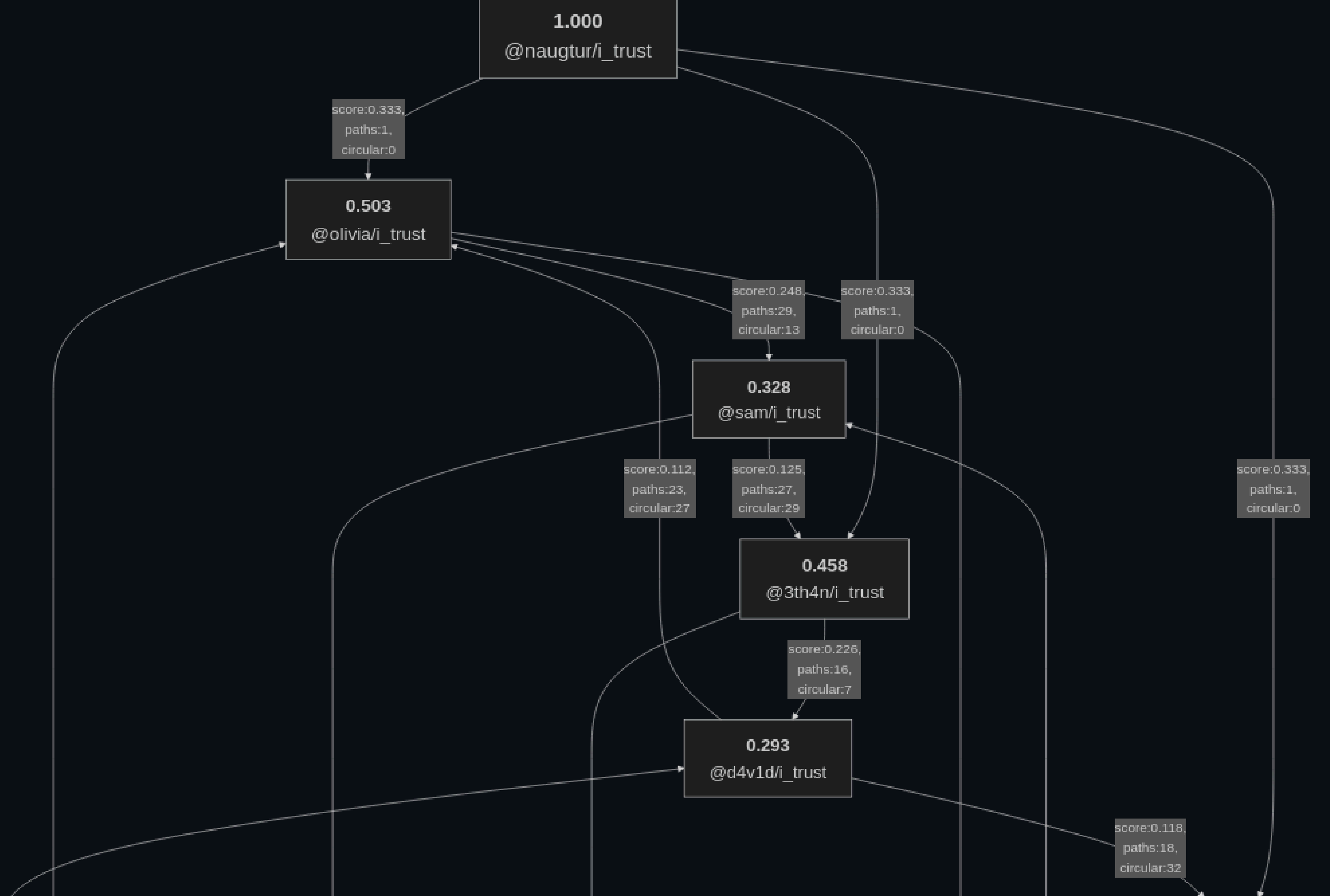
Assertions

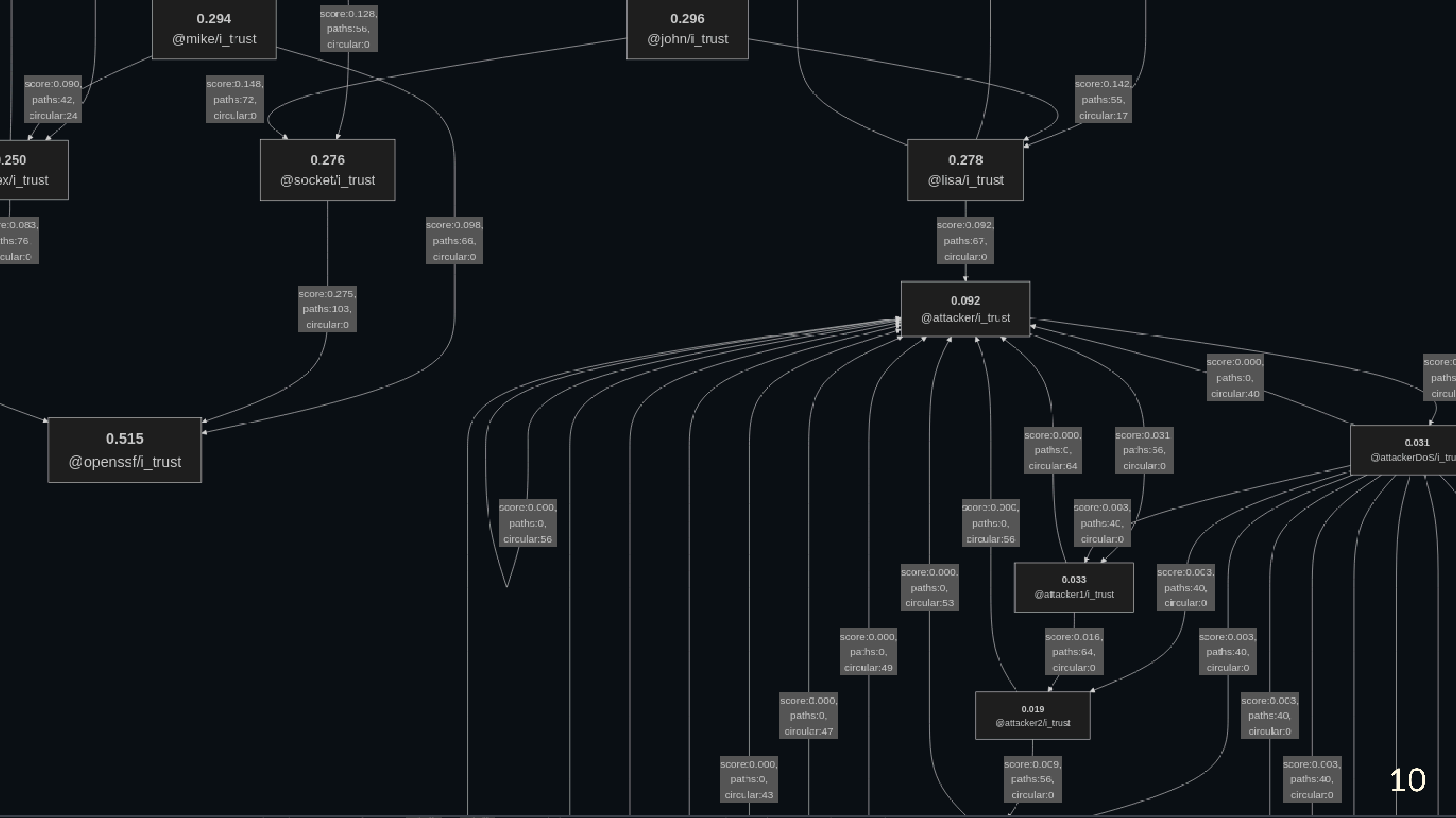
- Stored in JSON files or endpoints
- Can endorse (+1) or dispute (-1) claims about packages
- Include subject, claim, and trust score
- Easily queried and consumed by tools

Trust graph

- computed scores and the trickle-down effect on the whole graph
- attack resistance

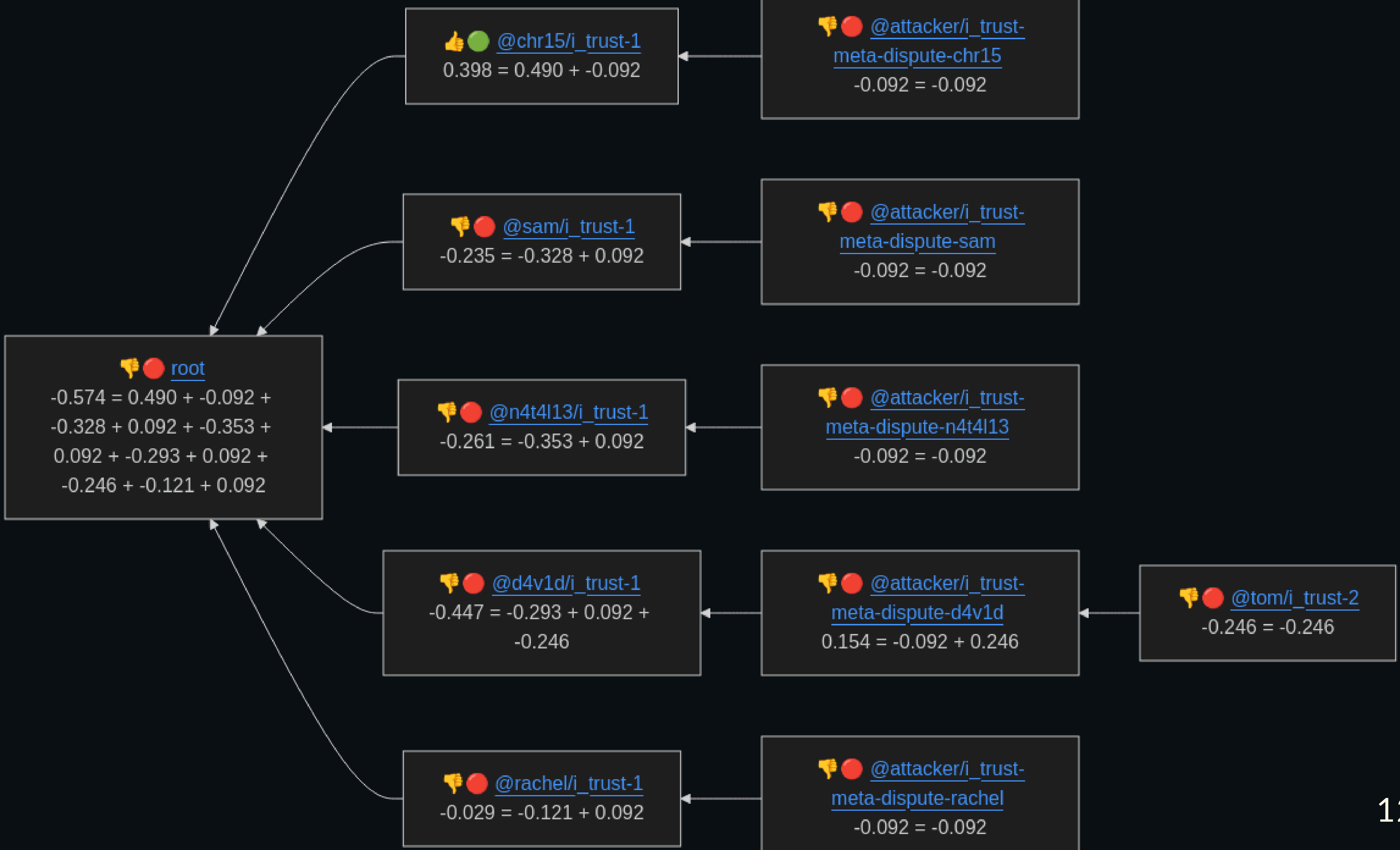
> “ Fragments of the trust graph computation visualized below ”


1.000
@naugtur/i_trust
score:0.333,
paths:1,
circular:0
0.503
@olivia/i_trust
score:0.248,
paths:29,
circular:13
score:0.333,
paths:1,
circular:0
0.328
@sam/i_trust
score:0.112,
paths:23,
circular:27
score:0.125,
paths:27,
circular:29
score:0.333,
paths:1,
circular:0
0.458
@3th4n/i_trust
score:0.226,
paths:16,
circular:7
0.293
@d4v1d/i_trust
score:0.118,
paths:18,
circular:32


0.294
@mike/i_trust
score:0.128,
paths:56,
circular:0
0.296
@john/i_trust
score:0.090,
paths:42,
circular:24
score:0.148,
paths:72,
circular:0
score:0.142,
paths:55,
circular:17
.250
ex/i_trust
0.276
@socket/i_trust
0.278
@lisa/i_trust
re:0.083,
ths:76,
cular:0
score:0.098,
paths:66,
circular:0
score:0.092,
paths:67,
circular:0
score:0.275,
paths:103,
circular:0
0.092
@attacker/i_trust
score:0.000,
paths:0,
circular:40
score:(
paths
circul
0.515
@openssf/i_trust
score:0.000,
paths:0,
circular:64
score:0.031,
paths:56,
circular:0
0.031
@attackerDoS/i_tru
score:0.000,
paths:0,
circular:56
score:0.000,
paths:0,
circular:56
score:0.003,
paths:40,
circular:0
score:0.000,
paths:0,
circular:53
0.033
@attacker1/i_trust
score:0.003,
paths:40,
circular:0
score:0.000,
paths:0,
circular:49
score:0.016,
paths:64,
circular:0
score:0.003,
paths:40,
circular:0
score:0.000,
paths:0,
circular:47
0.019
@attacker2/i_trust
score:0.003,
paths:40,
circular:0
score:0.000,
paths:0,
circular:43
score:0.009,
paths:56,
circular:0
score:0.003,
paths:40,
circular:0

Assertions matching and weight

- query for assertions about a subject
- weight to represent how much you trust the peers listed
- summarize to one sentiment score



👍🟢 @chr15/i_trust-1
0.398 = 0.490 + -0.092

👎🔴 @attacker/i_trust-meta-dispute-chr15
-0.092 = -0.092

👎🔴 @sam/i_trust-1
-0.235 = -0.328 + 0.092

👎🔴 @attacker/i_trust-meta-dispute-sam
-0.092 = -0.092

👎🔴 root
-0.574 = 0.490 + -0.092 + -0.328 + 0.092 + -0.353 + 0.092 + -0.293 + 0.092 + -0.246 + -0.121 + 0.092

👎🔴 @n4t4l13/i_trust-1
-0.261 = -0.353 + 0.092

👎🔴 @attacker/i_trust-meta-dispute-n4t4l13
-0.092 = -0.092

👎🔴 @d4v1d/i_trust-1
-0.447 = -0.293 + 0.092 + -0.246

👎🔴 @attacker/i_trust-meta-dispute-d4v1d
0.154 = -0.092 + 0.246

👎🔴 @tom/i_trust-2
-0.246 = -0.246

👎🔴 @rachel/i_trust-1
-0.029 = -0.121 + 0.092

👎🔴 @attacker/i_trust-meta-dispute-rachel
-0.092 = -0.092

Applications and Impact

1. Filter npm audit results based on trusted opinions
2. Reduce noise from unnecessary vulnerability reports
3. Empower the community to collaboratively dismiss bogus CVEs
4. Avoid creating a centralized mess with no authority willing to moderate it

Resources

project: github.com/naugtur/trust-graph

trust graph example
sentiment visualized