UNVEILING THE BITCOIN ALPHA TRUST NETWORK.

A NETWORK SCIENCE APPROACH

BITCOIN DATASET.🔗

WHO-TRUSTS-WHOM NETWORK OF PEOPLE WHO TRADE USING BITCOIN ON THE PLATFORM BITCOIN ALPHA. MEMBERS OF BITCOIN ALPHA RATE OTHER MEMBERS IN A SCALE OF -10 (TOTAL DISTRUST) TO +10 (TOTAL TRUST) AS USERS ARE ANONYMOUS.

{ SOURCE, TARGET, RATING, TIME }
NODES : 3,783
EDGES : 24,186
RANGE OF WEIGHTS : -10 TO +10

DELIVERABLE 1.

WHERE DISTRUST LIVES?
HOW IT SPREADS?
WHO DRIVES IT?
WHEN IT EXPLODES?
HOW YOU CAN STOP IT?

WE ARE SIMULATING THE SPREAD OF DISTRUST (A KIND OF “INFECTION”) OVER A TRUST NETWORK, LIKE A SOCIAL NETWORK WHERE USERS RATE EACH OTHER POSITIVELY OR NEGATIVELY. START WITH A FEW SEED NODES (INITIALLY “INFECTED” PEOPLE), AND THE INFECTION SPREADS TO OTHERS OVER TIME — BASED ON HOW MUCH THEY DISTRUST THEIR NEIGHBOURS.

ALPHA (α) IS A THRESHOLD:

A NODE BECOMES ”INFECTED” (STARTS DISTRUSTING OTHERS) IF THE SUM OF INCOMING NEGATIVE TRUST CROSSES THIS α VALUE. IN SIMPLE TERMS:

- IF α = 0.1, THEN A NODE BECOMES INFECTED IF IT GETS “ENOUGH” NEGATIVE VIBES FROM NEIGHBORS — JUST 10% DISTRUST FROM PEOPLE IT LISTENS TO IS ENOUGH.

THINK OF IT LIKE: “IF 1 IN 10 OF MY FRIENDS DISTRUST SOMEONE, I’LL START DISTRUSTING THEM TOO.”

DISTRUST INFECTION GROWTH OVER TIME

WHAT IT SHOWS

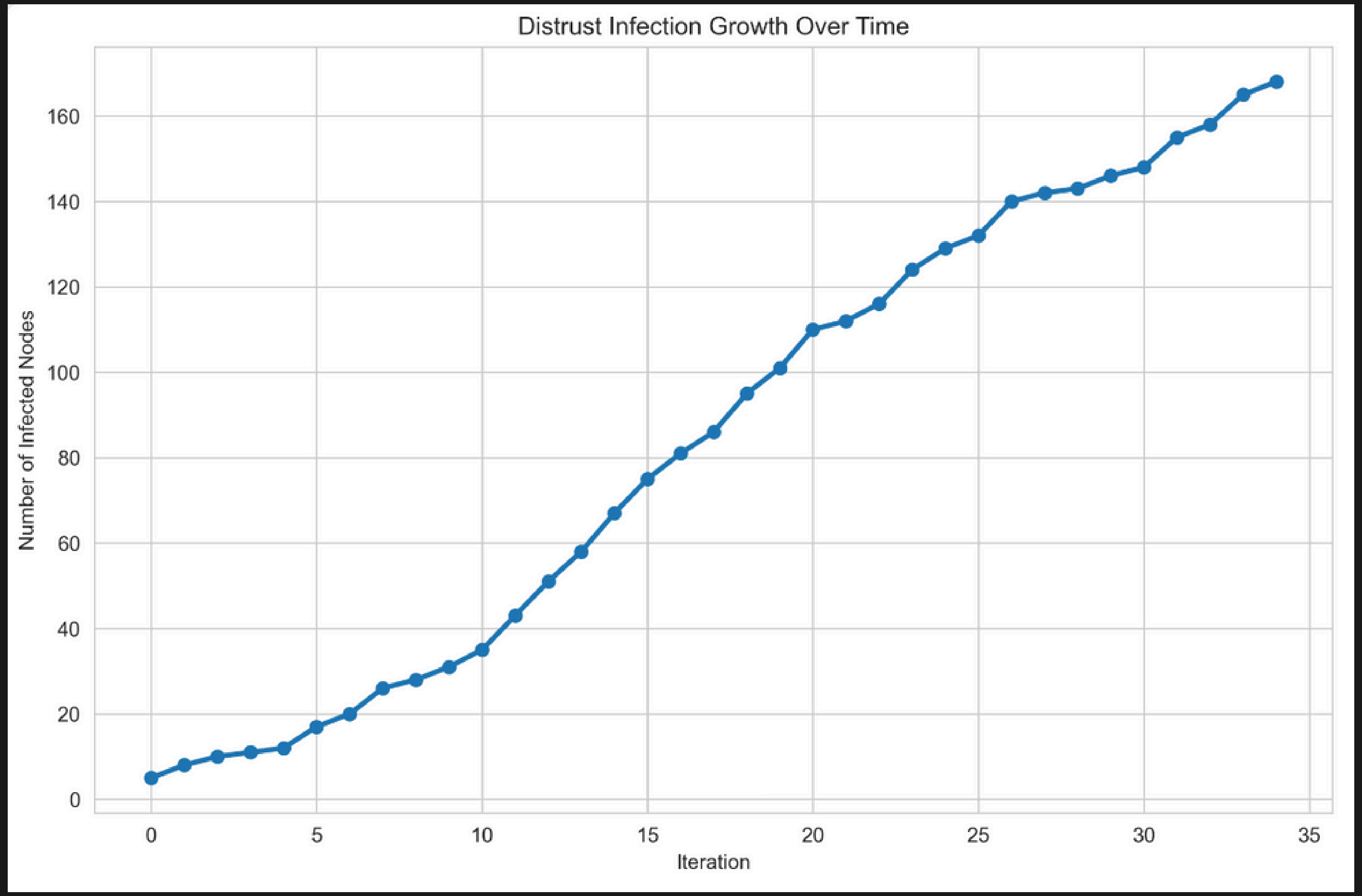
A LINE GRAPH OF TOTAL INFECTED PEOPLE AFTER EACH ROUND. STARTS AROUND 5 NODES (SEED NODES), SLOWLY CLIMBS TO 168 NODES OVER 35 ROUNDS.

SIMPLE MEANING

AT FIRST, DISTRUST SPREADS SLOWLY. THEN IT SPEEDS UP BETWEEN ROUND 6–15 (MANY NEW PEOPLE GET INFECTED). THEN IT SLOWS AGAIN AND STOPS AROUND ROUND 35.

WHY?

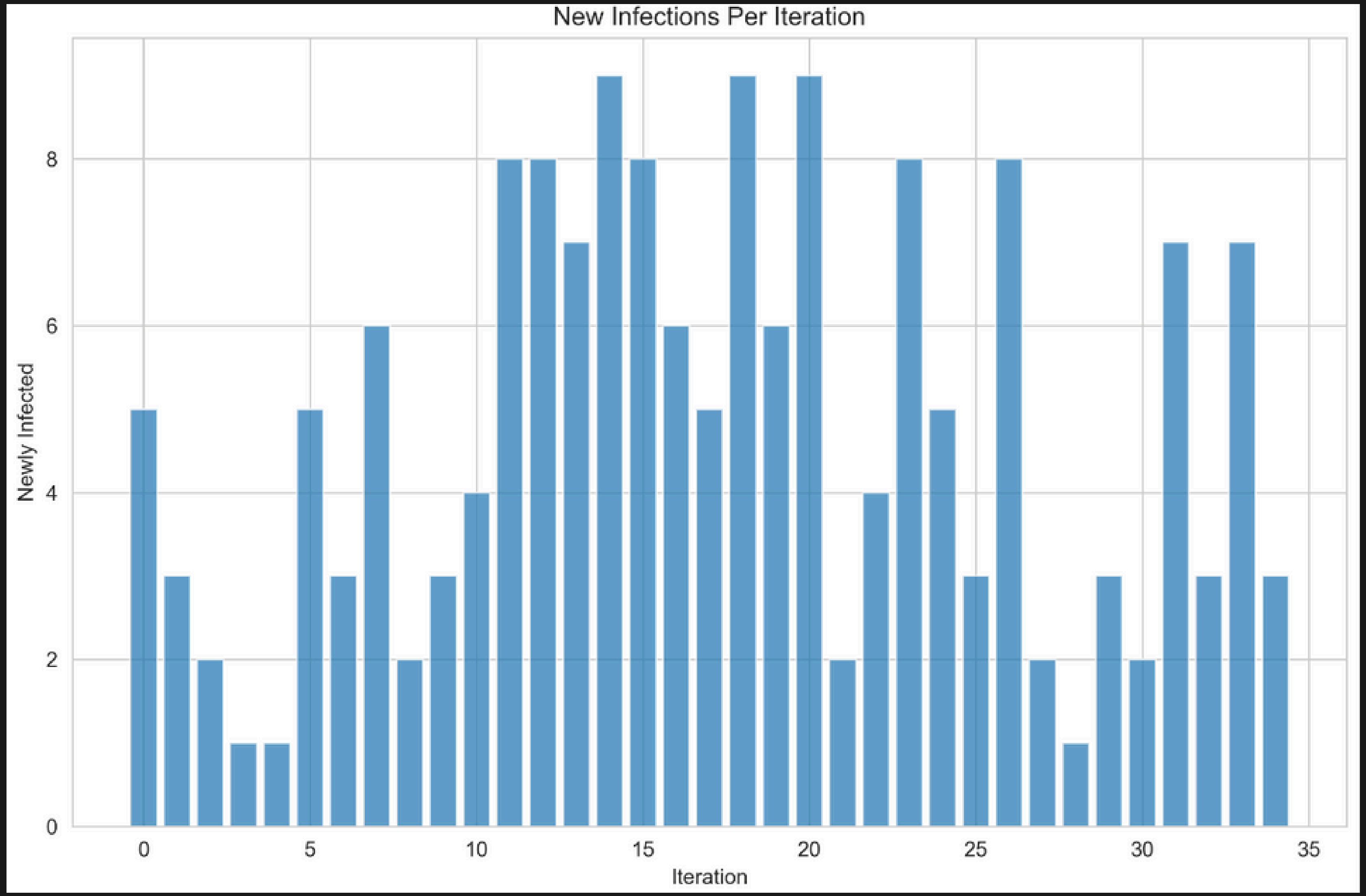
BECAUSE AFTER A POINT, THERE ARE NO MORE EASY TARGETS — MOST PEOPLE ARE TOO TRUSTING, OR TOO FAR FROM INFECTED ONES.



NEW INFECTIONS PER ITERATION

WHAT IT SHOWS

A BAR CHART — HOW MANY NEW PEOPLE GET INFECTED IN EACH ROUND. BIG SPIKES AT ROUND 14 AND 20: MOST NEW INFECTIONS HAPPEN THERE. AFTER ROUND 26,FEW GET INFECTED.



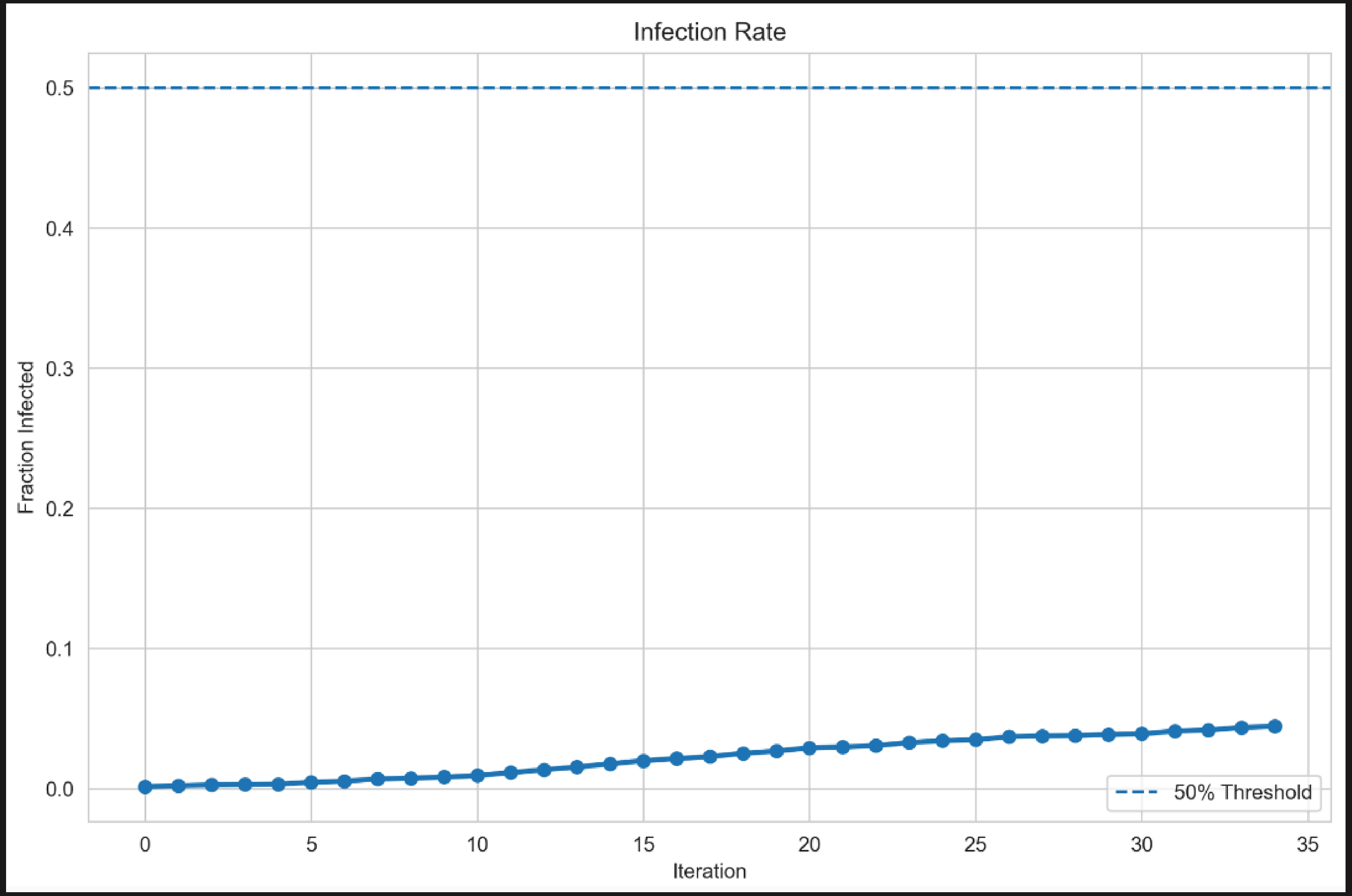
SIMPLE MEANING

DISTRUST SPREADS IN BURSTS, LIKE “WAVES”. A GROUP OF PEOPLE GETS INFECTED, WHICH TRIGGERS THE NEXT BATCH. EVENTUALLY, IT DIES DOWN.

WHY?

BECAUSE INFECTED PEOPLE ONLY REACH NEW PEOPLE THROUGH CERTAIN BRIDGES IN THE NETWORK.

INFECTION RATE (FRACTION INFECTED)



WHAT IT SHOWS

LINE GRAPH OF HOW MANY PEOPLE ARE INFECTED AS A PERCENTAGE OF THE TOTAL NETWORK. FINAL NUMBER AROUND 4.5% OF THE TOTAL 3,783 NODES. THE DOTTED LINE AT 50% CHECKS IF THE INFECTION WENT VIRAL.

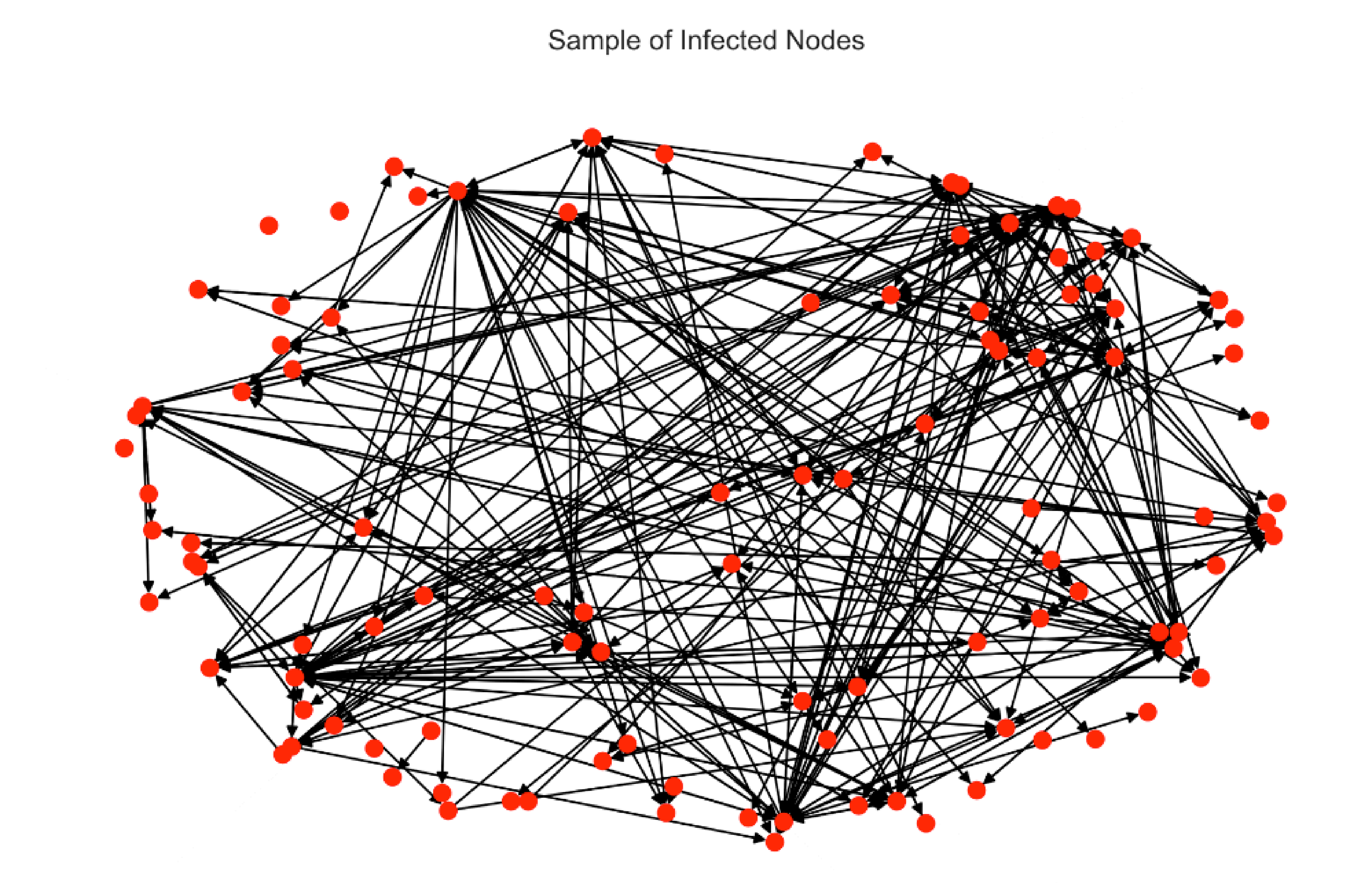
SIMPLE MEANING

THE SPREAD NEVER GOES BIG — IT STAYS LOCAL. IT NEVER INFECTS EVEN HALF THE NETWORK.

WHY?

BECAUSE ALPHA = 0.1 ISN’T AGGRESSIVE, AND MOST PEOPLE AREN’T IN CONTACT WITH ENOUGH DISTRUST TO CROSS THE THRESHOLD.

INFECTED NODE SUBGRAPH



WHAT IT SHOWS

A SPRING-LAYOUT DRAWING OF 100 INFECTED NODES, COLOURED RED, SHOWING THAT INFECTED PEOPLE FORM SMALL CLUSTERS, NOT ONE GIANT CLUSTER.

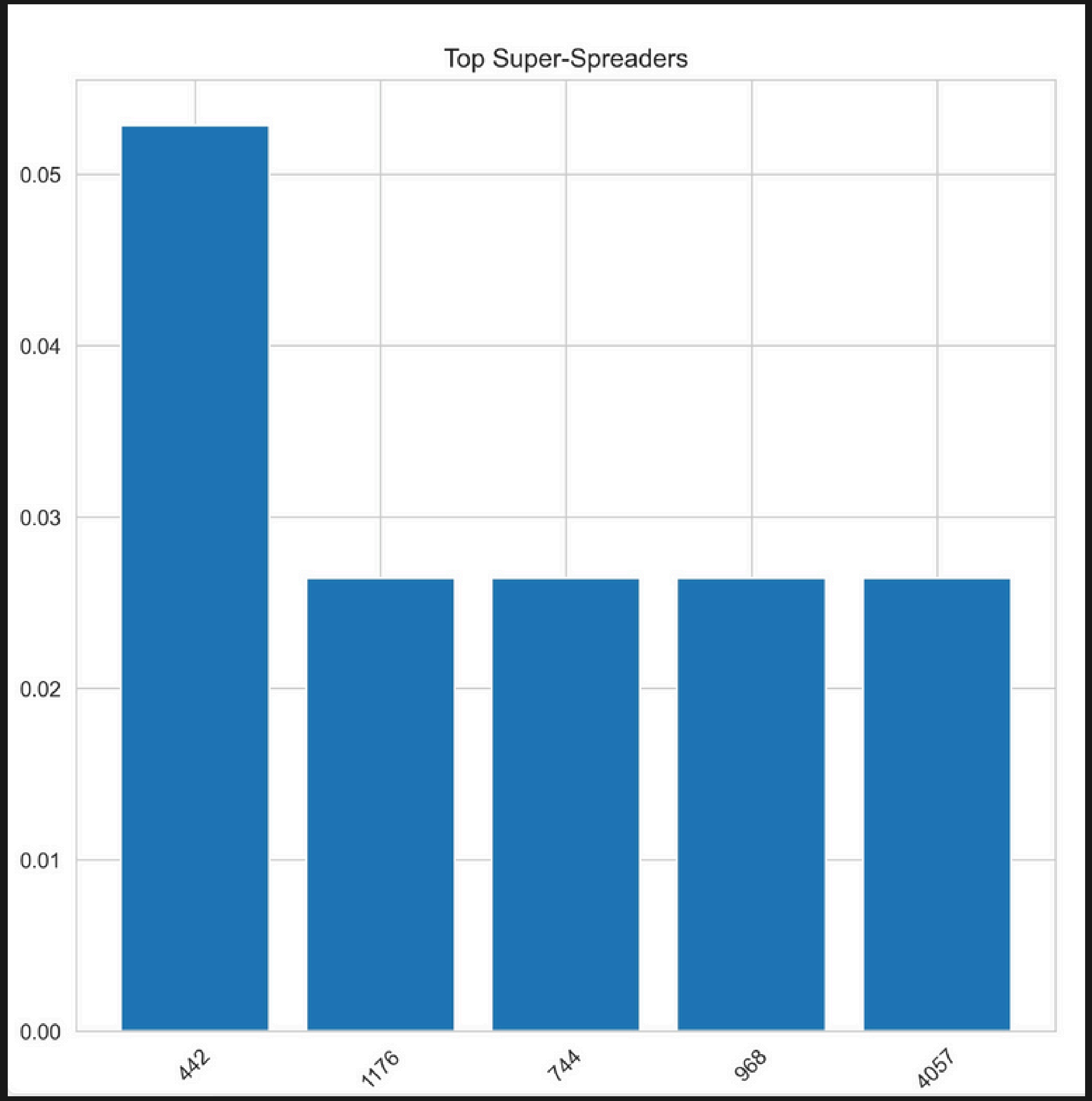
SIMPLE MEANING

DISTRUST SPREADS IN LOCAL POCKETS. THERE'S NO GIANT CONNECTED GROUP OF INFECTED, JUST SMALL DISCONNECTED GROUPS.

WHY?

BECAUSE THE NETWORK HAS MANY CLUSTERS, AND ONLY SOME CLUSTERS HAVE ENOUGH DISTRUST TO ACTIVATE.

A BAR CHART OF THE TOP 5 SUPER-SPREADERS — THE NODES THAT, WHEN SEEDED ALONE, CAUSED THE LARGEST NUMBER OF INFECTIONS.



WHAT EACH BAR SHOWS

HOW MANY NODES THAT SEED EVENTUALLY INFECTED (PERCENTAGE OF THE TOTAL NETWORK THAT IS).

SIMPLE MEANING

“IF WE INFECT ONLY NODE A, HOW FAR DOES THE DISTRUST SPREAD?” FOR SOME NODES, IT BARELY SPREADS. BUT FOR THESE TOP 5, IT SPREADS TO TENS OR HUNDREDS OF OTHERS.

FOR EXAMPLE

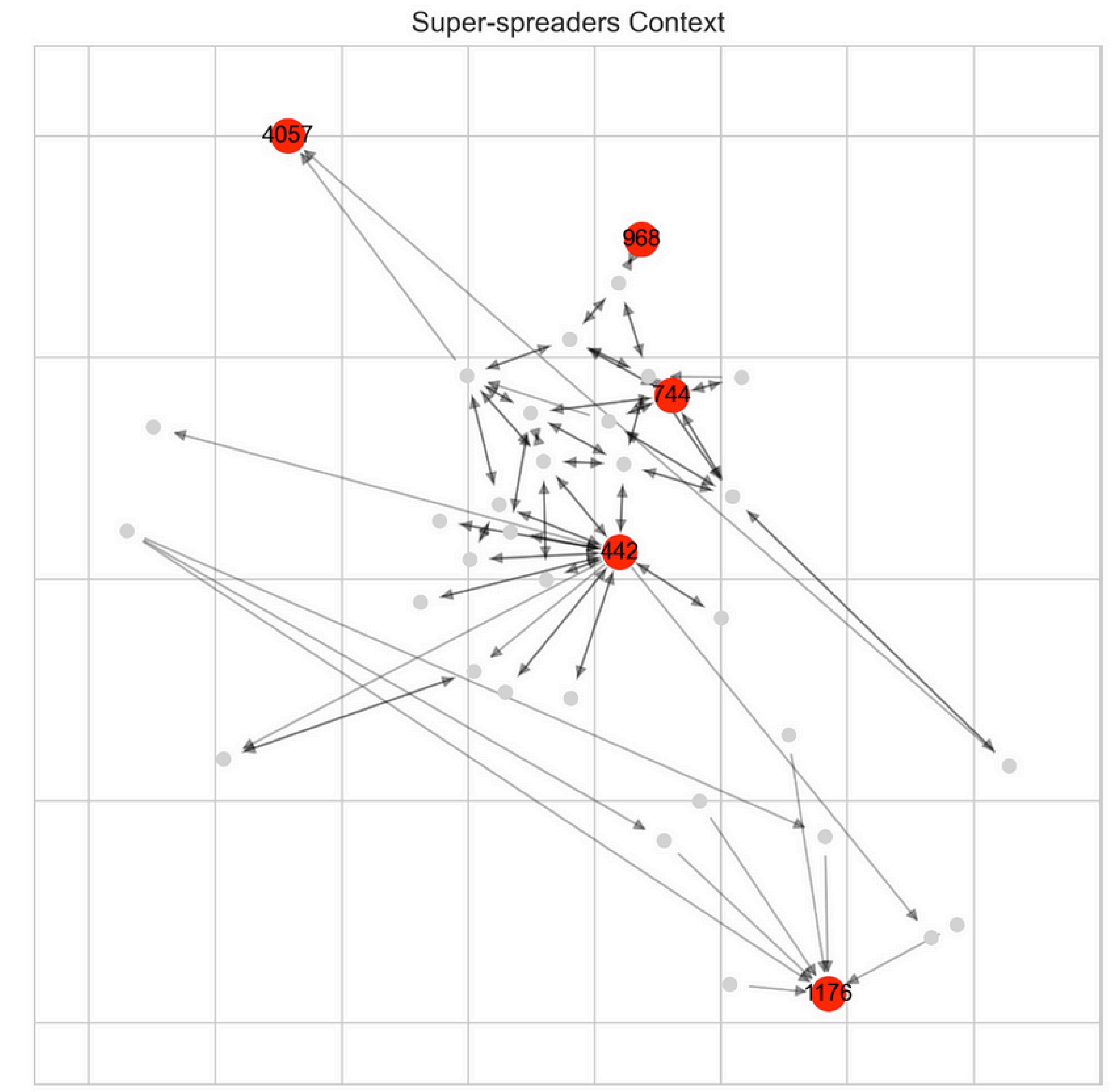
NODE A ALONE MIGHT INFECT 85 PEOPLE (OUT OF 3,783), OR 2.2%. NODE B MIGHT CAUSE 50 PEOPLE TO GET INFECTED. SO, SOME NODES ARE WAY MORE DANGEROUS THAN OTHERS IN SPREADING DISTRUST.

SUPER-SPREADERS CONTEXT

WHAT IT SHOWS

A NETWORK SUBGRAPH THAT ZOOMS IN ON THESE 5 TOP SUPER-SPREADERS AND THEIR NEIGHBORHOODS.

- RED NODES = THE 5 SUPER-SPREADERS.
- GRAY NODES = THEIR NEIGHBORS (PEOPLE THEY INFLUENCE OR ARE INFLUENCED BY).
- ARROWS = DIRECTION OF NEGATIVE TRUST (WHO DISTRUSTS WHOM).



SIMPLE MEANING:

“WHERE DO THESE SUPER-SPREADERS SIT IN THE NETWORK, AND WHY DO THEY HAVE SO MUCH INFLUENCE?” TURNS OUT:

- THEY’RE IN HIGHLY CONNECTED ZONES.
- THEY HAVE LOTS OF OUTGOING NEGATIVE EDGES TO OTHER PARTS OF THE NETWORK.
- THEY ACT AS BRIDGES BETWEEN OTHERWISE DISCONNECTED PARTS OF THE NETWORK.

THEY’RE DANGEROUS, THEY CAN START MULTIPLE DISTRUST CASCADES FROM A 1 PLACE.

INTUITION

THE AVERAGE PERSON IN THE NETWORK MIGHT HAVE ONLY LOCAL INFLUENCE. BUT A FEW KEY PEOPLE (SUPER-SPREADERS) ARE STRATEGICALLY PLACED TO AFFECT LARGE PARTS OF THE NETWORK. THESE PEOPLE SIT AT CROSSROADS, THEY LINK MANY COMMUNITIES AND HAVE STRONG NEGATIVE INFLUENCE. IF THEY START DISTRUSTING, THEY CAN TRIGGER MULTIPLE WAVES OF SPREADING DISTRUST.

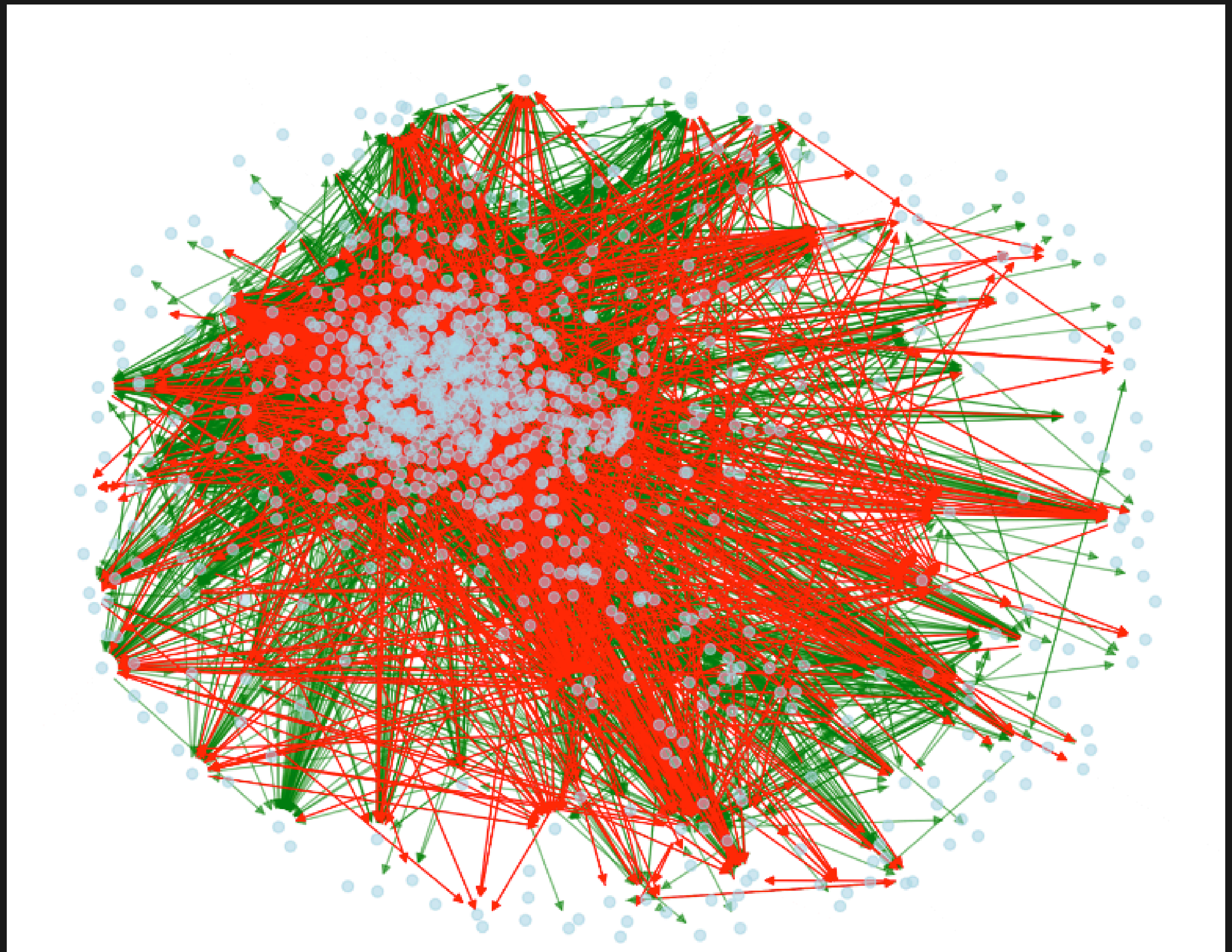
IMPLICATION

“IF YOU WANT TO STOP THE SPREAD OF DISTRUST, WATCH THESE FEW NODES CAREFULLY.” THEY ARE CRITICAL FOR MONITORING (E.G., SOCIAL PLATFORMS, MODERATION SYSTEMS). REMOVING OR NEUTRALISING THEM COULD DRAMATICALLY REDUCE THE RISK OF LARGE-SCALE CASCADES. THEY’RE LIKE FIRE STARTERS — TAKE THEM OUT, AND THE FOREST DOESN’T BURN.

TRUST VS DISTRUST DISTRIBUTION

WHAT IT SHOWS

A VISUAL MAP OF PART OF THE NETWORK, CONNECTED NODES ARE PULLED TOGETHER. GREEN EDGES ARE TRUSTING CONNECTIONS & RED EDGES ARE DISTRUSTING ONES.



INTUITION

TRUST FORMS TIGHT COMMUNITIES, WITH USERS MOSTLY CONNECTED WITHIN THEIR GROUP. DISTRUST LINKS JUMP BETWEEN GROUPS, SUCH BRIDGES ARE RARE BUT POWERFUL, SUGGESTING THAT DISTRUST CAN TRAVEL ACROSS THE NETWORK, EVEN IF IT’S NOT COMMON.

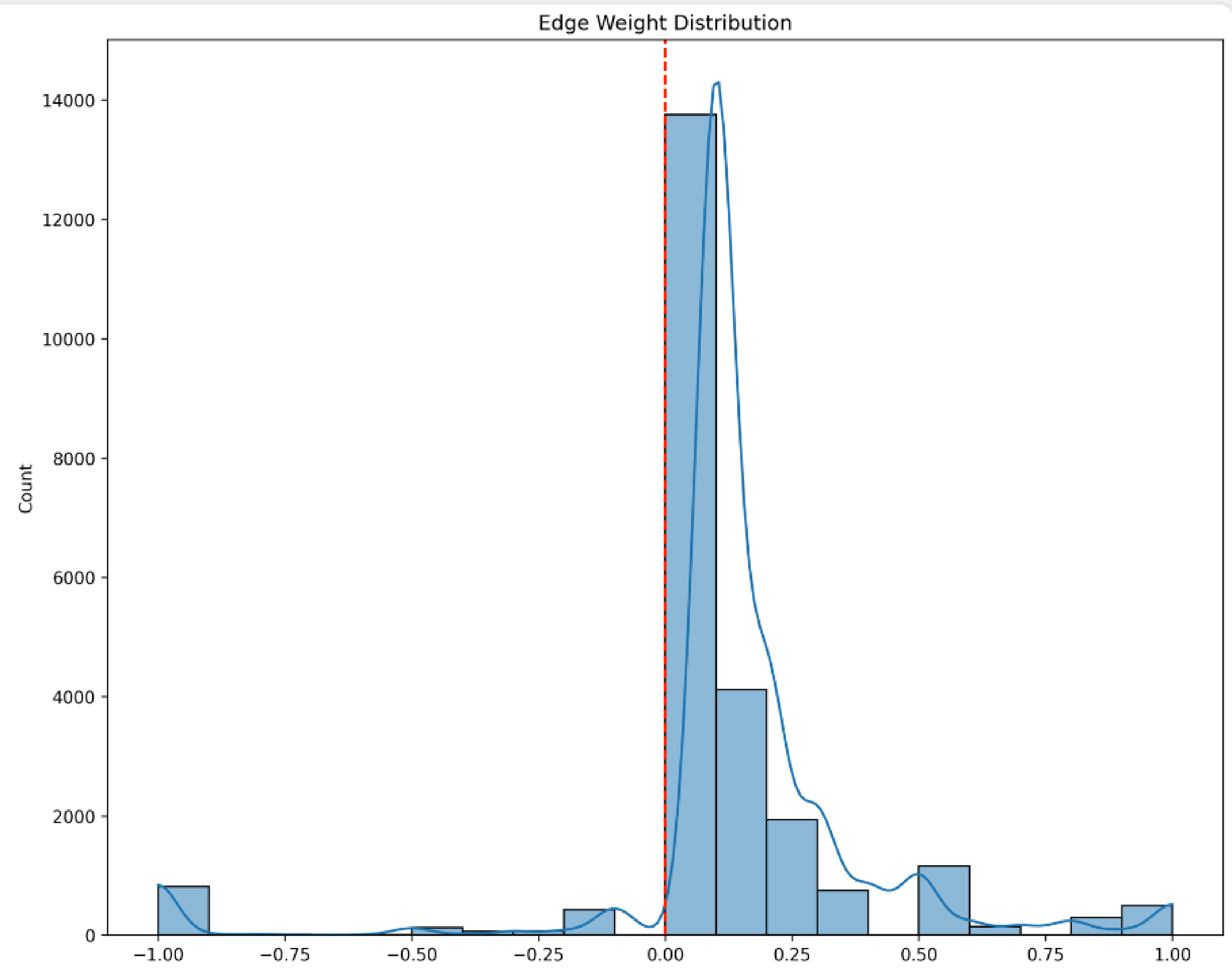
IMPLICATIONS

EVEN RARE DISTRUST CAN HAVE HUGE REACH BECAUSE OF HOW IT LINKS DISTANT PARTS. A FEW KEY DISTRUST LINKS CAN BREAK THE NETWORK APART OR SPREAD NEGATIVITY FAST. USEFUL FOR PLATFORMS TRYING TO DETECT EARLY SIGNS OF CONFLICT, POLARIZATION, OR MISINFORMATION.

EDGE WEIGHT DISTRIBUTION

WHAT IT SHOWS

HISTOGRAM OF EDGE WEIGHTS (FROM -1 TO +1), I.E., HOW STRONGLY PEOPLE TRUST/DISTRUST EACH OTHER. MOST EDGES ARE SLIGHTLY POSITIVE (MILD TRUST); VERY FEW ARE STRONGLY NEGATIVE.



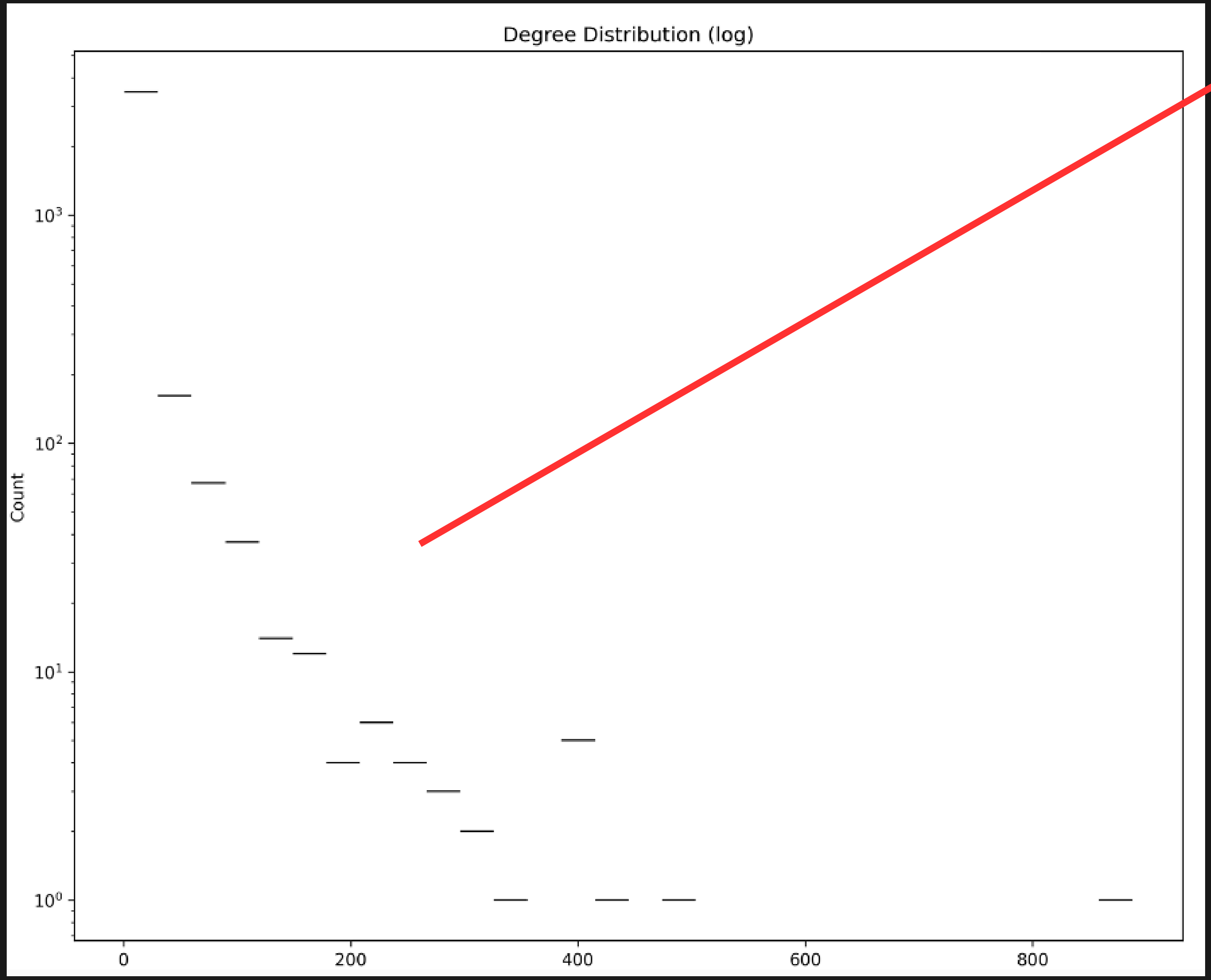
INTUITION

- MILD TRUST IS THE DEFAULT — USERS TRUST OTHERS, BUT NOT VERY STRONGLY.
- STRONG DISTRUST IS RARE, BUT THOSE FEW NEGATIVE RELATIONSHIPS STAND OUT AND CAN BE DISRUPTIVE.

IMPLICATION

- THE SYSTEM IS MOSTLY STABLE, AS MOST RELATIONSHIPS ARE POSITIVE.
- BUT SMALL, INTENSE DISTRUST LINKS CAN DESTABILISE TRUST-BASED SYSTEMS (LIKE REVIEWS, RATINGS, OR SOCIAL FEEDBACK).

NODE DEGREE DISTRIBUTION



POWER LAW

WHAT IT SHOWS

SHOWS HOW MANY CONNECTIONS EACH USER HAS. MOST USERS HAVE FEW CONNECTIONS; A FEW HAVE HUNDREDS (LOG EXAGGERATES RARE HIGH VALUES).

INTUITION

IT'S A "SCALE-FREE" NETWORK: A FEW HUB USERS ARE HIGHLY CONNECTED, WHILE MOST ARE NOT. THESE HUBS ARE VERY INFLUENTIAL, FOR BETTER (SPREADS TRUST) OR WORSE (SPREADS DISTRUST).

IMPLICATION

INFLUENTIAL USERS (HIGH-DEGREE NODES) ARE CRUCIAL, IF THEY GO ROGUE OR GET COMPROMISED, THE WHOLE NETWORK IS AFFECTED. PLATFORMS CAN TARGET INTERVENTIONS/RECOMMENDATIONS BASED ON USER CENTRALITY. TRUST SHOULD BE WEIGHTED CAREFULLY FOR "HUB" USERS TO PREVENT UNFAIR AMPLIFICATION.

FAIRNESS SCORE DISTRIBUTION

What it shows

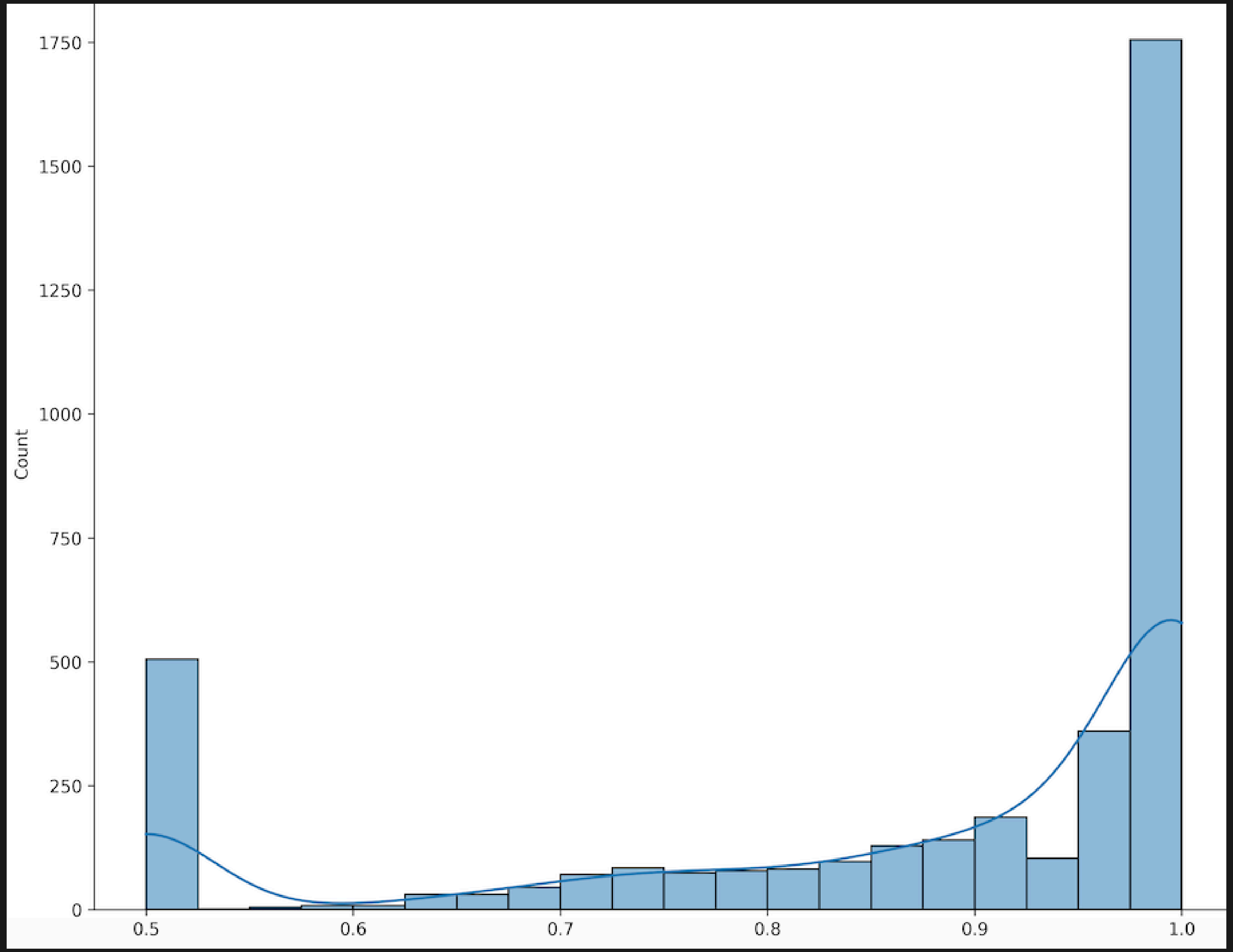
How fair/consistent each user is in their trust ratings (score between 0.1 and 1.0). Most users are fair (score near 1.0), but a few are very unfair.

Intuition

Most people rate others in a reliable and predictable way But a few users give very inconsistent or erratic ratings, which can break trust systems.

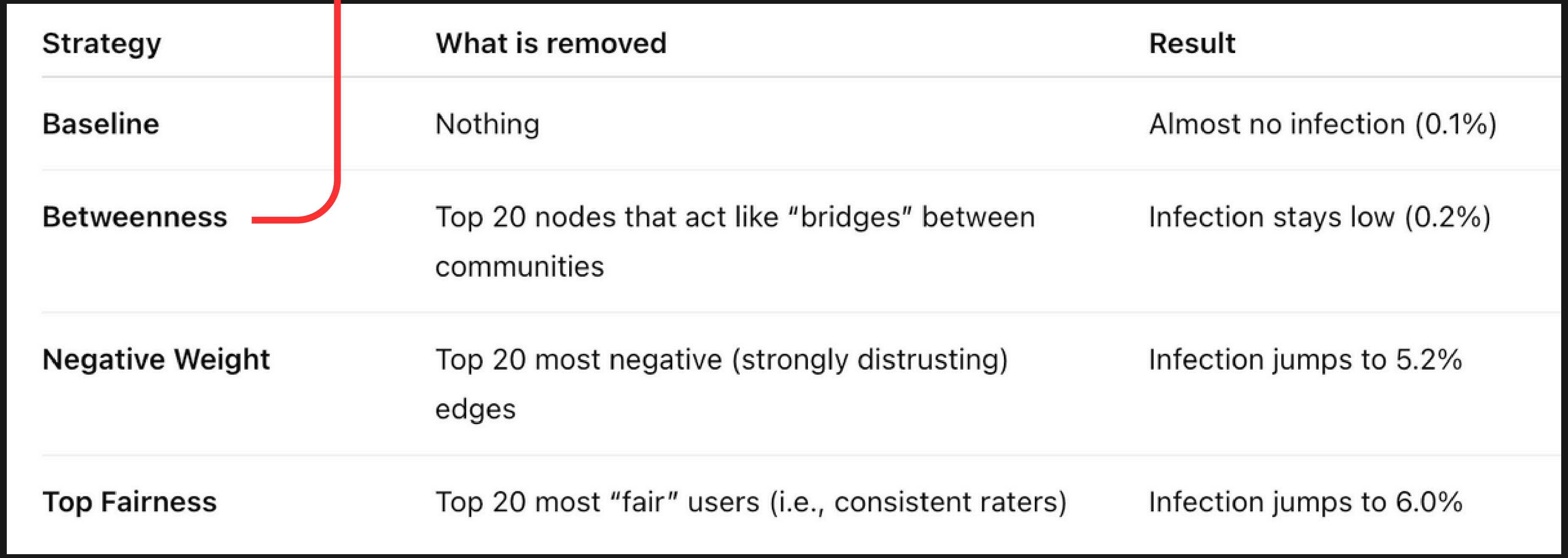
Implication

Unfair users can manipulate the network with biased feedback. Even a few unfair users can skew perceptions, especially if they are well-connected. Platforms should flag low-fairness users for review or give their ratings less weight.

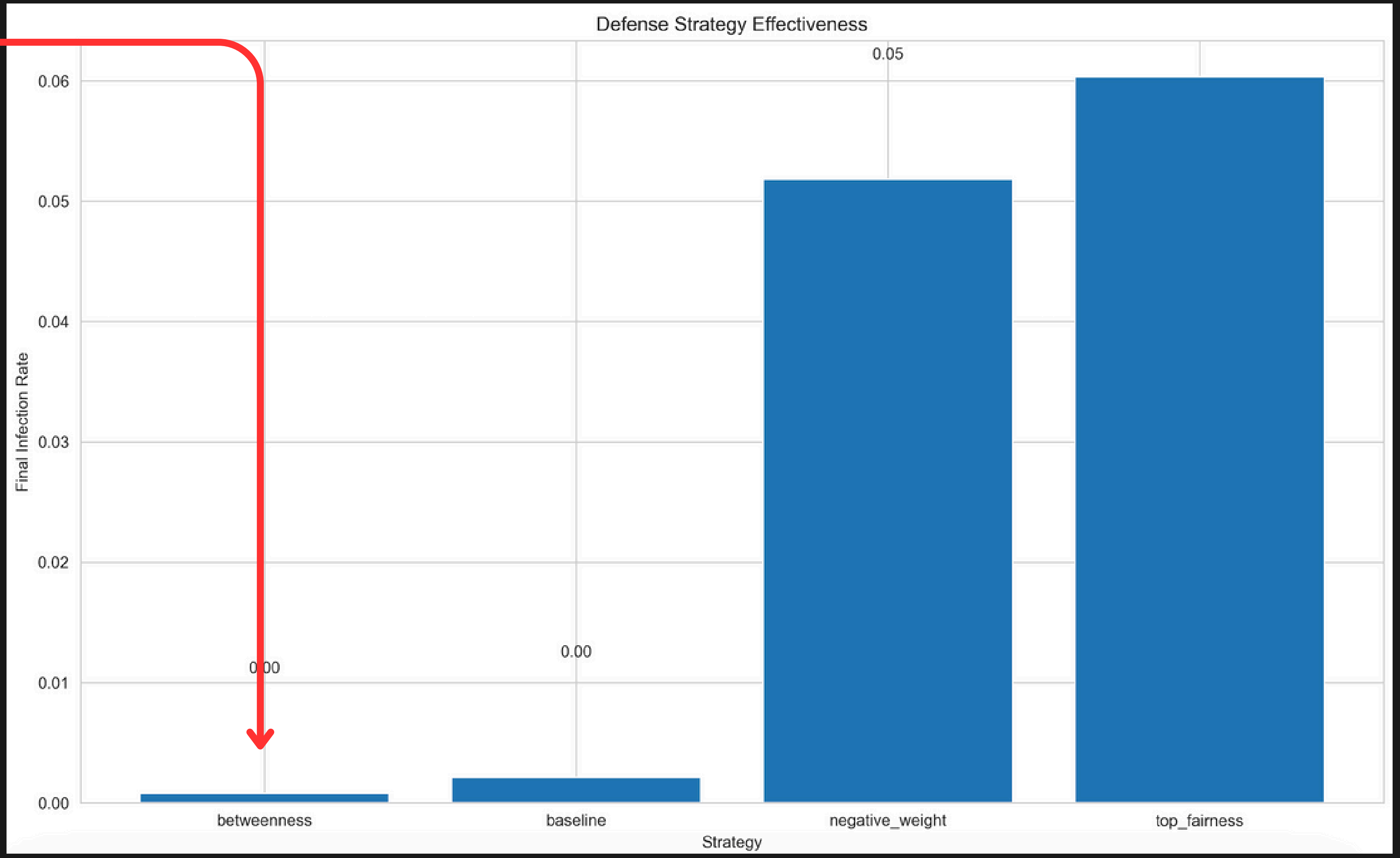


DEFENCE STRATEGIES

THIS GRAPH SHOWS HOW DISTRUST (INFECTION) SPREADS THROUGH A NETWORK, AND HOW WELL DIFFERENT STRATEGIES STOP IT. BASELINE: NO INTERVENTION → ONLY ~0.1% OF THE NETWORK GETS "INFECTED" (MEANING, DISTRUST SPREADS VERY LITTLE). THEN WE TEST THREE DEFENSE STRATEGIES BY REMOVING CERTAIN NODES/EDGES BEFORE RUNNING THE SIMULATION AGAIN.



Strategy	What is removed	Result
Baseline	Nothing	Almost no infection (0.1%)
Betweenness	Top 20 nodes that act like "bridges" between communities	Infection stays low (0.2%)
Negative Weight	Top 20 most negative (strongly distrusting) edges	Infection jumps to 5.2%
Top Fairness	Top 20 most "fair" users (i.e., consistent raters)	Infection jumps to 6.0%



✅ BETWEENNESS REMOVAL:

"CUT THE BRIDGES, AND DISTRUST CAN'T SPREAD FAR."

NODES WHICH SIT AT IMPORTANT CONNECTION POINTS BETWEEN DIFFERENT COMMUNITIES ARE REMOVED. REMOVING THEM CUTS OFF THE PATHWAYS DISTRUST WOULD NORMALLY USE TO TRAVEL FAR. THINK OF THEM LIKE BORDER CHECKPOINTS — IF THEY'RE REMOVED, PEOPLE CAN'T CROSS BORDERS EASILY.

❌ NEGATIVE EDGE REMOVAL:

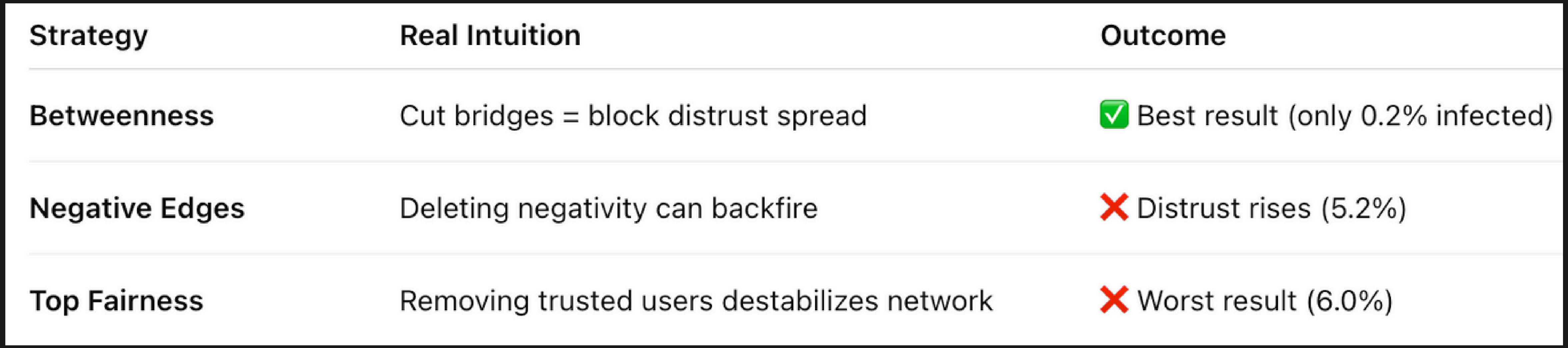
"REMOVING LOUD COMPLAINTS MAKES SMALL ROOMS ECHO LOUDER."

REMOVES EDGES WITH STRONGEST DISTRUST. SOUNDS GOOD, BUT IT BACKFIRES: NOW COMMUNITIES ARE MORE ISOLATED. DISTRUST THEN BUILDS UP INSIDE GROUPS, SINCE THERE'S NO OUTLET OR BALANCE. THINK OF THEM, LIKE JUST DELETING NEGATIVITY WITHOUT STRUCTURAL THINKING CAN AMPLIFY INTERNAL TOXICITY.

❌ TOP FAIRNESS REMOVAL:

“FIRING THE REFEREES LETS CHAOS TAKE OVER THE GAME.”

REMOVES USERS WHO ARE MOST CONSISTENT AND RELIABLE IN THEIR RATINGS. THIS MAKES THE SYSTEM LESS STABLE, BECAUSE NOW ONLY ERRATIC, UNFAIR RATERS REMAIN. INFECTION SPREADS MORE BECAUSE THE SYSTEM LOSES ITS MOST TRUSTWORTHY VOICES. THINK OF THIS LIKE, REMOVING FAIR USERS UNDERMINES THE WHOLE TRUST SYSTEM — THEY ARE THE GLUE HOLDING IT TOGETHER.



Strategy	Real Intuition	Outcome
Betweenness	Cut bridges = block distrust spread	✅ Best result (only 0.2% infected)
Negative Edges	Deleting negativity can backfire	❌ Distrust rises (5.2%)
Top Fairness	Removing trusted users destabilizes network	❌ Worst result (6.0%)

DON’T JUST REMOVE THINGS THAT “LOOK BAD” (LIKE UNFAIR PEOPLE OR NEGATIVE COMMENTS). INSTEAD, REMOVE THOSE WHO CONNECT COMMUNITIES IF YOU WANT TO STOP PROBLEMS FROM SPREADING.

DELIVERABLE 2.

GROUP USERS
INTO BEHAVIOUR
BASED CATEGORIES

METHODOLOGY

INTUITION

TRUST ISN'T A SIMPLE METRIC YOU CAN MEASURE WITH A RULER—IT'S A MULTI-LAYERED PHENOMENON INVOLVING NETWORK CONNECTIONS, USER BEHAVIORS, AND RISK ATTITUDES. TO UNPACK IT, WE NEED A SOPHISTICATED TOOLKIT THAT DIGS INTO BOTH THE "WHO" AND THE "HOW" OF TRUST IN THE NETWORK.

FINDINGS

- NETWORK FEATURE EXTRACTION: COMPUTED METRICS LIKE DEGREE CENTRALITY (HOW MANY CONNECTIONS A USER HAS), BETWEENNESS CENTRALITY (HOW OFTEN A USER BRIDGES DIFFERENT PARTS OF THE NETWORK), AND TRUST-SPECIFIC FEATURES (E.G., AVERAGE TRUST GIVEN/RECEIVED).
- DIMENSIONALITY REDUCTION: APPLIED TECHNIQUES LIKE PCA (PRINCIPAL COMPONENT ANALYSIS) AND T-SNE (T-DISTRIBUTED STOCHASTIC NEIGHBOUR EMBEDDING) TO SIMPLIFY COMPLEX DATA INTO VISUALISABLE PATTERNS, REVEALING CLUSTERS OF SIMILAR USERS.
- CLUSTER ANALYSIS: USED CLUSTERING ALGORITHMS (E.G., K-MEANS OR HIERARCHICAL CLUSTERING) TO GROUP USERS INTO 5 DISTINCT SEGMENTS BASED ON THEIR NETWORK ROLES AND TRUST BEHAVIOURS.

IMPLICATION

IT'S A SCALABLE FRAMEWORK, DECENTRALISED NETWORKS (ETHEREUM, SOCIAL PLATFORMS, OR E-COMMERCE MARKETPLACES) CAN ADOPT IT TO UNCOVER HIDDEN USER PATTERNS, IMPROVE SYSTEM DESIGN (LIKE BETTER RECOMMENDATION ENGINES), OR SPOT ANOMALIES.

POWER USERS/HUBS (CLUSTER 0)

INTUITION

THINK OF POWER USERS AS THE CENTRAL HUBS IN A BUSY AIRPORT—PLANES (OR IN THIS CASE, TRUST AND TRANSACTIONS) FLOW THROUGH THEM TO REACH OTHER DESTINATIONS. THEY'RE THE CONNECTORS WHO KEEP THE NETWORK HUMMING.

FINDINGS

- SIZE: 158 USERS, MAKING UP 4.18% OF THE NETWORK.
- CONNECTIVITY: HIGHLY ACTIVE WITH AN AVERAGE OF 51.8 OUTGOING CONNECTIONS (TRUST GIVEN) AND 49.3 INCOMING CONNECTIONS (TRUST RECEIVED).
- TRUST: THEY'RE NET TRUST RECIPIENTS—MORE USERS TRUST THEM THAN THEY TRUST OTHERS.
- RISK-TAKING: SHOW A CONSISTENTLY HIGH RISK TOLERANCE (MEAN: 0.92, LOW VARIATION), MEANING THEY'RE COMFORTABLE ENGAGING IN VOLATILE OR UNCERTAIN TRANSACTIONS.
- CENTRALITY: HIGH BETWEENNESS AND EIGENVECTOR CENTRALITY SCORES INDICATE THEY OCCUPY STRATEGIC POSITIONS, LINKING OTHERWISE DISCONNECTED PARTS OF THE NETWORK.

IMPLICATION

THESE USERS ARE THE BACKBONE OF NETWORK STABILITY. PLATFORMS CAN USE THEM TO BROADCAST CRITICAL UPDATES OR SECURITY ALERTS QUICKLY ACROSS THE NETWORK, POSITION THEM AS TRUSTED INTERMEDIARIES FOR HIGH-STAKES TRANSACTIONS, REDUCING PERCEIVED RISK FOR OTHERS AND TAP THEM AS BETA TESTERS FOR NEW FEATURES, LEVERAGING THEIR ACTIVE ENGAGEMENT AND INFLUENCE.

CASUAL USERS (CLUSTER 1)

INTUITION

CASUAL USERS ARE THE EVERYDAY FOLKS WHO DIP THEIR TOES INTO THE NETWORK BUT DON'T DIVE IN HEADFIRST. THEY'RE LIKE WEEKEND SHOPPERS AT A MARKET—PRESENT IN LARGE NUMBERS BUT NOT DEEPLY INVESTED.

FINDINGS

- SIZE: 3,186 USERS, A WHOPPING 84.24% OF THE NETWORK.
- CONNECTIVITY: MINIMAL ENGAGEMENT WITH AN AVERAGE OF 3.5 OUTGOING AND 3.8 INCOMING CONNECTIONS.
- TRUST: NEUTRAL TRUST EXCHANGE—THEY GIVE AND RECEIVE TRUST AT SIMILAR LEVELS, SHOWING NO STRONG BIAS.
- RISK-TAKING: VARIABLE RISK ATTITUDES (MEAN: 0.83, HIGH VARIATION), MEANING SOME ARE CAUTIOUS WHILE OTHERS ARE MORE ADVENTUROUS.
- CENTRALITY: LOW CENTRALITY SCORES PLACE THEM ON THE NETWORK'S PERIPHERY.

IMPLICATION

SINCE THEY'RE THE MAJORITY, PLATFORMS MUST CATER TO THEM BY DESIGNING INTUITIVE, BEGINNER-FRIENDLY INTERFACES TO LOWER THE ENTRY BARRIER, OFFERING EDUCATIONAL TOOLS (TUTORIALS ON TRUST RATINGS) TO BUILD CONFIDENCE, INTRODUCING INCENTIVES (SMALL REWARDS FOR ACTIVITY) TO NUDGE THEM TOWARD DEEPER ENGAGEMENT, POTENTIALLY TURNING THEM INTO POWER USERS OVER TIME.

SUPER CONNECTORS/AUTHORITIES (CLUSTER 2)

INTUITION

SUPER CONNECTORS ARE THE ROCKSTARS OF THE NETWORK, A GROUP WHOSE INFLUENCE FAR EXCEEDS THEIR SMALL NUMBERS. THEY'RE THE TRENDSETTERS AND OPINION LEADERS EVERYONE WATCHES.

FINDINGS

- SIZE: JUST 15 USERS, OR 0.40% OF THE NETWORK.
- CONNECTIVITY: EXTRAORDINARY REACH WITH 208.7 OUTGOING AND 180.7 INCOMING AVG. CONNECTIONS.
- TRUST: THEY ACCUMULATE SIGNIFICANT TRUST, RECEIVING FAR MORE THAN THEY GIVE.
- RISK-TAKING: STRATEGICALLY HIGH RISK TOLERANCE (MEAN: 0.88, LOW VARIATION), SUGGESTING CALCULATED BOLDNESS.
- CENTRALITY: SKY-HIGH CENTRALITY SCORES MAKE THEM AUTHORITATIVE FIGURES.
- THREAT DETECTION: ACTIVELY FLAG POTENTIAL THREATS, CONTRIBUTING TO NETWORK SECURITY.

IMPLICATIONS

THEIR OUTSIZED INFLUENCE MAKES THEM GAME-CHANGERS. PLATFORMS CAN MODEL TRUST ALGORITHMS AFTER THEIR BEHAVIOUR (E.G., WEIGHTING THEIR RATINGS MORE HEAVILY), RECRUIT THEM TO SHAPE NETWORK CULTURE/NORMS AND USE THEM AS COMMUNITY MODERATORS OR EARLY ADOPTERS FOR NEW TOOLS, AMPLIFYING ADOPTION.

TRUSTING PERIPHERAL USERS (CLUSTER 3)

INTUITION

THESE USERS ARE THE WELCOMING COMMITTEE—OPEN, TRUSTING, AND EAGER TO CONNECT, EVEN IF THEY'RE NOT DEEPLY EMBEDDED IN THE NETWORK. THEY HELP THE NETWORK GROW.

FINDINGS

- SIZE: 322 USERS, OR 8.51% OF THE NETWORK.
- CONNECTIVITY: LIMITED ACTIVITY WITH 2.7 OUTGOING AND 2.7 INCOMING CONNECTIONS.
- TRUST: EXTREMELY GENEROUS, GIVING AN AVERAGE TRUST RATING OF 5.95 (ON A SCALE WHERE 10 IS MAX).
- RISK-TAKING: NEARLY MAXIMAL RISK TOLERANCE (MEAN: 0.998, ALMOST NO VARIATION), SHOWING FEARLESS ENGAGEMENT.
- CENTRALITY: LOW CENTRALITY KEEPS THEM ON THE EDGES.

IMPLICATIONS

THEIR OPENNESS IS A DOUBLE-EDGED SWORD. PLATFORMS SHOULD PROTECT THEM FROM SCAMS WITH SAFEGUARDS LIKE TRANSACTION LIMITS OR FRAUD ALERTS, LEVERAGE THEM IN GROWTH CAMPAIGNS (E.G., REFERRAL BONUSES) TO ATTRACT NEW USERS AND EDUCATE THEM ON RISKS, ENSURING THEIR TRUST DOESN'T MAKE THEM EASY TARGETS.

SKEPTICS/VIGILANTES (CLUSTER 4)

INTUITION

SKEPTICS ARE THE NETWORK'S WATCHDOGS—CAUTIOUS, CRITICAL, AND QUICK TO CALL OUT ANYTHING SUSPICIOUS. THEY'RE THE GUARDIANS WHO KEEP EVERYONE HONEST.

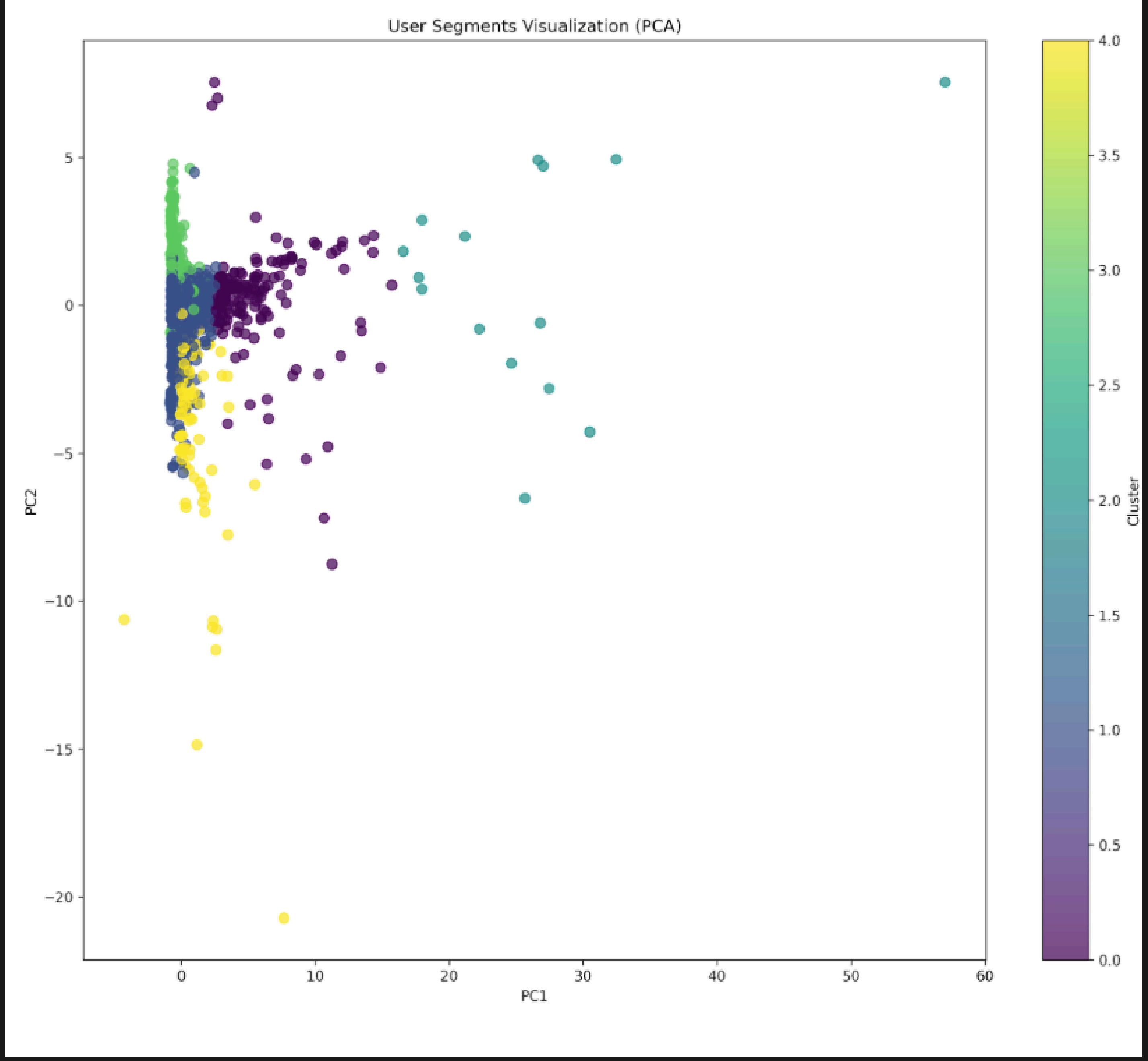
FINDINGS

- SIZE: 101 USERS, OR 2.67% OF THE NETWORK.
- CONNECTIVITY: MODERATE ACTIVITY WITH 7.7 OUTGOING AND 8.0 INCOMING CONNECTIONS.
- TRUST: NET NEGATIVE TRUST ORIENTATION (AVERAGE TRUST GIVEN: -1.11), MEANING THEY DISTRUST MORE THAN THEY TRUST.
- RISK-TAKING: LOWEST RISK TOLERANCE (MEAN: 0.65), REFLECTING A CONSERVATIVE APPROACH.
- TRUST VOLATILITY: EXTREMELY HIGH (MEAN: 35.52), INDICATING SHARP, BINARY TRUST DECISIONS (EITHER FULLY TRUSTING OR FULLY DISTRUSTING).
- THREAT DETECTION: HIGH RATES OF NEGATIVE TRUST SHOW THEY'RE ACTIVE IN FLAGGING RISKS.

IMPLICATION

THEIR VIGILANCE IS A SECURITY ASSET. PLATFORMS CAN EQUIP THEM WITH ADVANCED REPORTING TOOLS TO EFFICIENTLY FLAG THREATS, ANALYSE THEIR FEEDBACK TO REFINE SECURITY ALGORITHMS OR DETECT EMERGING SCAMS AND MONITOR THEIR ACTIVITY TO BALANCE THEIR SKEPTICISM WITH FAIRNESS, PREVENTING OVER-FLAGGING.

PCA MAP VISUALISATION ANALYSIS



THIS MAP IS CREATED USING PCA (PRINCIPAL COMPONENT ANALYSIS), A CLEVER WAY TO TAKE MESSY, COMPLICATED DATA AND TURN IT INTO A SIMPLE 2D PICTURE.

HORIZONTAL LINE (PC1): THE ACTIVITY STREET

THIS LINE IS ALL ABOUT HOW MUCH SOMEONE PARTICIPATES—QUIET VISITORS ON THE LEFT, SOCIAL STARS ON THE RIGHT.

VERTICAL LINE (PC2): THE TRUST LADDER

NOW THINK OF THIS AS A LADDER SHOWING HOW PEOPLE FEEL ABOUT THE PLATFORM, UP MEANS WARM AND TRUSTING VIBES, DOWN MEANS A COOLER, MORE GUARDED ATTITUDE.

SUPER CONNECTORS (YELLOW)

THESE ARE THE ROCKSTARS! THEY'RE CAMPED OUT ON THE FAR RIGHT (PC1 AROUND 50-60), SUPER ACTIVE AND LINKED UP WITH EVERYONE. SOME CLIMB A BIT UP THE TRUST LADDER TOO, SHOWING THEY'RE NOT JUST BUSY BUT BELOVED.

SKEPTICS (TEAL)

THESE FOLKS ARE ALL OVER THE PLACE, FROM PC1 0 TO 40 AND PC2 -10 TO 5. THEY'RE ACTIVE IN DIFFERENT WAYS BUT OFTEN HANG LOWER ON THE TRUST LADDER—THINK OF THEM AS THE CAUTIOUS OBSERVERS, KEEPING AN EYE OUT RATHER THAN JUMPING IN HEADFIRST.

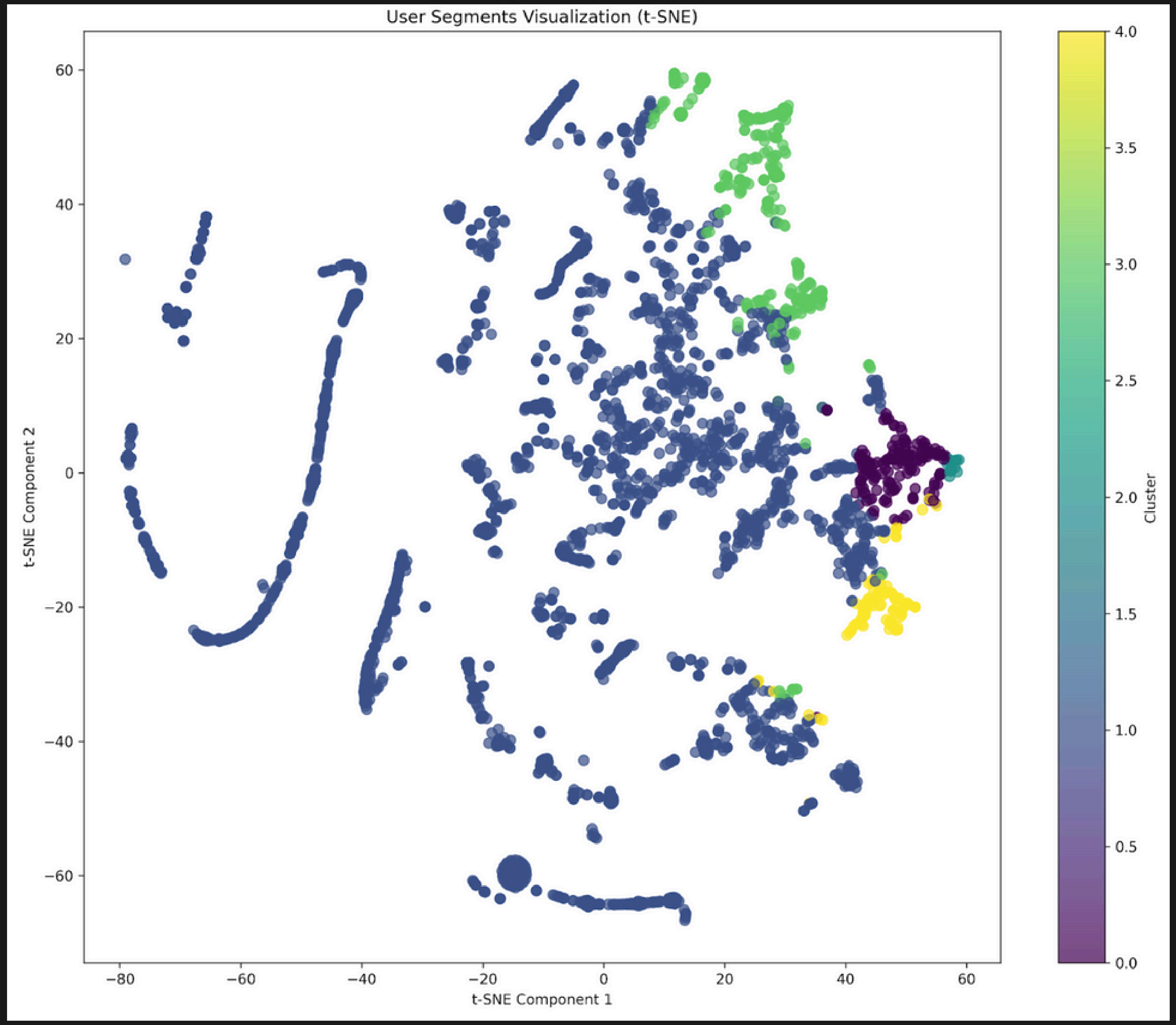
POWER USERS (PURPLE)

THIS CREW STICKS TOGETHER IN A TIGHT HUDDLE AROUND PC1 10-20 AND PC2 -5 TO 5. THEY'RE PRETTY ACTIVE AND RELIABLE—LIKE VOLUNTEERS WHO KEEP THE COMMUNITY RUNNING SMOOTHLY. A FEW WANDER OFF, SHOWING SOME VARIETY, BUT THEY'RE A STEADY BUNCH.

MAJORITY OF USERS (BLUE)

THE BIGGEST GROUP CLUSTERS RIGHT IN THE MIDDLE, NEAR PC1 AND PC2 AROUND 0. THESE ARE THE EVERYDAY FOLKS—LIKE PEOPLE WHO WALK THROUGH THE PARK BUT DON'T ORGANIZE THE PICNIC. THEY'RE NOT TOO ACTIVE AND FEEL PRETTY NEUTRAL ABOUT TRUST.

T-SNE MAP VISUALISATION ANALYSIS



HORIZONTAL ROAD (T-SNE COMPONENT 1)
RUNS FROM -80 ON THE LEFT TO 60 ON THE RIGHT.
VERTICAL ROAD (T-SNE COMPONENT 2)
GOES FROM -60 AT THE BOTTOM TO 60 AT THE TOP.

ON THE RIGHT SIDE, THERE’S A COLORFUL BAR GOING FROM DEEP PURPLE (0.0) TO BRIGHT YELLOW (4.0). THIS BAR IS LIKE A CLUE—IT SHOWS US HOW TIGHT OR DISTINCT THE GROUPS ARE, KIND OF LIKE A ”FRIENDSHIP STRENGTH” METER. THE MAP IS DOTTED WITH COLORFUL POINTS, EACH ONE REPRESENTING A USER. THESE POINTS CLUMP TOGETHER IN PATTERNS THAT REVEAL THE HIDDEN STORIES.

NEIGHBOURHOODS BIG AND SMALL

BIG CLUSTERS OF POINTS—LIKE THE DARK BLUE BLOBS ALL OVER THE MAP—ARE THE MAIN NEIGHBORHOODS. BUT ZOOM IN, AND YOU'LL SPOT SMALLER GROUPS INSIDE THEM. FOR EXAMPLE, UP IN THE UPPER-MIDDLE PART, BRIGHT GREEN DOTS (LET'S CALL THEM "TRUSTING PERIPHERAL USERS") FORM LITTLE TIGHT-KNIT CIRCLES. THESE SMALLER GROUPS ACT SIMILAR WITHIN A BIGGER CROWD.

TRUST HIGHWAYS

CHECK OUT THE LONG, CURVY LINE OF BLUE DOTS STRETCHING FROM THE LOWER-LEFT (-60, -20) UP TO THE UPPER-MIDDLE (20, 40). IT LOOKS LIKE A CHAIN OR A PATH. THIS CHAIN SHOWS TRUST MOVING STEP-BY-STEP—ONE USER TRUSTS THE NEXT, WHO TRUSTS THE NEXT, LIKE A GAME OF TELEPHONE. IT'S A SEQUENCE OF CONNECTIONS LINKING PEOPLE ACROSS THE MAP.

THE FRIENDLY CONNECTORS

LOOK FOR LONE DOTS OR SMALL GROUPS SITTING BETWEEN THE BIG CLUSTERS. NEAR THE CENTER-RIGHT (AROUND 20, 0), YOU MIGHT SPOT PURPLE OR YELLOW DOTS BRIDGING A BLUE CLUSTER AND A GREEN ONE. THESE "BRIDGE USERS" ARE THE GLUE HOLDING THE TOWN TOGETHER. THEY'RE THE ONES WHO PASS NEWS, TRUST, OR IDEAS BETWEEN NEIGHBORHOODS THAT WOULDN'T OTHERWISE MEET.

TIGHT-KNIT FRIEND GROUPS

THOSE GREEN DOTS (TRUSTING PERIPHERAL USERS) IN THE UPPER-MIDDLE AND RIGHT-MIDDLE PARTS OF THE MAP ARE PACKED TIGHT, FORMING LITTLE ISLANDS. THE YELLOW DOTS DOWN IN THE LOWER-RIGHT (AROUND 20, -20) DO THE SAME. THESE TIGHT CLUSTERS MEAN STRONG BONDS—USERS WHO REALLY GET ALONG, TRUST EACH OTHER, AND MAYBE SHARE THE SAME HABITS. THEY'RE LIKE A CREW THAT'S ALWAYS ON THE SAME PAGE.

STRATEGIC IMPLICATIONS

SECURITY ENHANCEMENT

- LEVERAGE THE VIGILANCE OF SKEPTICS BY CREATING FORMAL FEEDBACK CHANNELS FOR THREAT REPORTING
- DEVELOP TAILORED SECURITY EDUCATION FOR HIGHLY TRUSTING USERS (CLUSTER 3)
- IMPLEMENT DIFFERENTIAL RISK SCORING THAT INCORPORATES SEGMENT-SPECIFIC TRUST PATTERNS
- MONITOR MIGRATION BETWEEN SEGMENTS AS AN EARLY WARNING FOR NETWORK HEALTH ISSUES

TRUST MECHANISM OPTIMIZATION

WEIGHT TRUST SCORES BASED ON USER SEGMENT TO IMPROVE RECOMMENDATION ACCURACY

CREATE COMPOUND TRUST METRICS UTILISING BOTH DIRECT RATINGS AND SEGMENT CHARACTERISTICS

DEVELOP SEGMENT-SPECIFIC TRUST THRESHOLDS FOR TRANSACTION APPROVALS

INCENTIVISE BALANCED DISTRIBUTION OF USER ARCHETYPES FOR OPTIMAL NETWORK HEALTH

USER EXPERIENCE DESIGN

- TAILOR INTERFACE ELEMENTS BASED ON RISK PROFILE AND SEGMENT CHARACTERISTICS
- PROVIDE SEGMENT-APPROPRIATE GUIDANCE AND TOOLS:
  - DECISION SUPPORT TOOLS FOR HIGH-VOLATILITY USERS
  - NETWORK VISUALIZATION FOR SUPER CONNECTORS
  - SIMPLIFIED INTERFACES FOR PERIPHERAL USERS
- ADVANCED FILTERING FOR SKEPTICS

OUTPUT CSV FILES

BRIDGE_USERS.CSV
SEGMENT_PROFILES.CSV
USER_PROFILES.CSV
USER_SEGMENTS_KMEANS.CSV
RISK_ATTITUDE_BY_SEGMENT.CSV

NOW WE ARE GOING TO PRESENT AN HTML WEBSITE WHICH IS GOING TO HELP YOU VISUALISE THE ANALYSIS DISCUSSED IN THIS DELIVERABLE !!

DELIVERABLE 3.

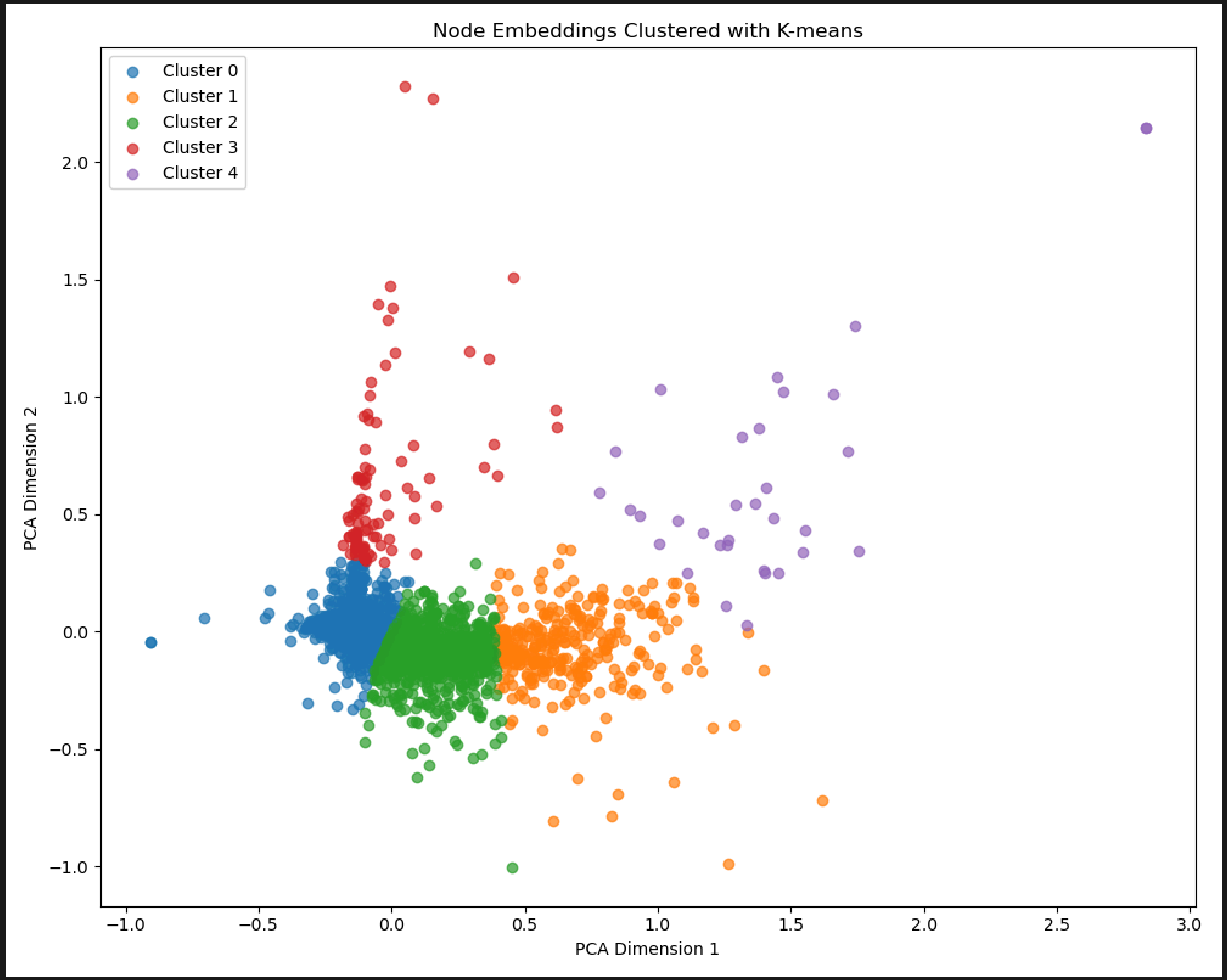
FIND THE ODD ONES OUT (ANOMALIES)

OUR ANALYSIS IDENTIFIED 2 PARTICULARLY ANOMALOUS CLUSTERS THAT EXHIBIT UNUSUAL INTERNAL TRUST PATTERNS COMPARED TO THEIR EXTERNAL RELATIONSHIPS:

Cluster ID	Size	Internal Trust Mean	External Trust Mean	Trust Ratio
1	248	3.56	1.75	2.03
4	76	6.23	3.18	1.96

CLUSTER 1 (248 USERS) SHOWS INTERNAL TRUST LEVELS THAT ARE APPROXIMATELY TWICE AS HIGH AS EXTERNAL TRUST LEVELS, SUGGESTING A POTENTIAL ”ECHO CHAMBER” EFFECT OR COORDINATED GROUP. CLUSTER 4 (76 USERS) DISPLAYS EVEN HIGHER INTERNAL TRUST VALUES WITH A SIMILAR RATIO TO EXTERNAL TRUST. THESE CLUSTERS MAY REPRESENT:

- COMMUNITY SUBGROUPS WITH STRONGER INTERNAL COHESION
- TRADING CIRCLES WITH ESTABLISHED TRUST RELATIONSHIPS
- POTENTIAL MANIPULATION RINGS ARTIFICIALLY BOOSTING INTERNAL TRUST SCORES



TEMPORAL ANOMALIES IN TRUST RATINGS

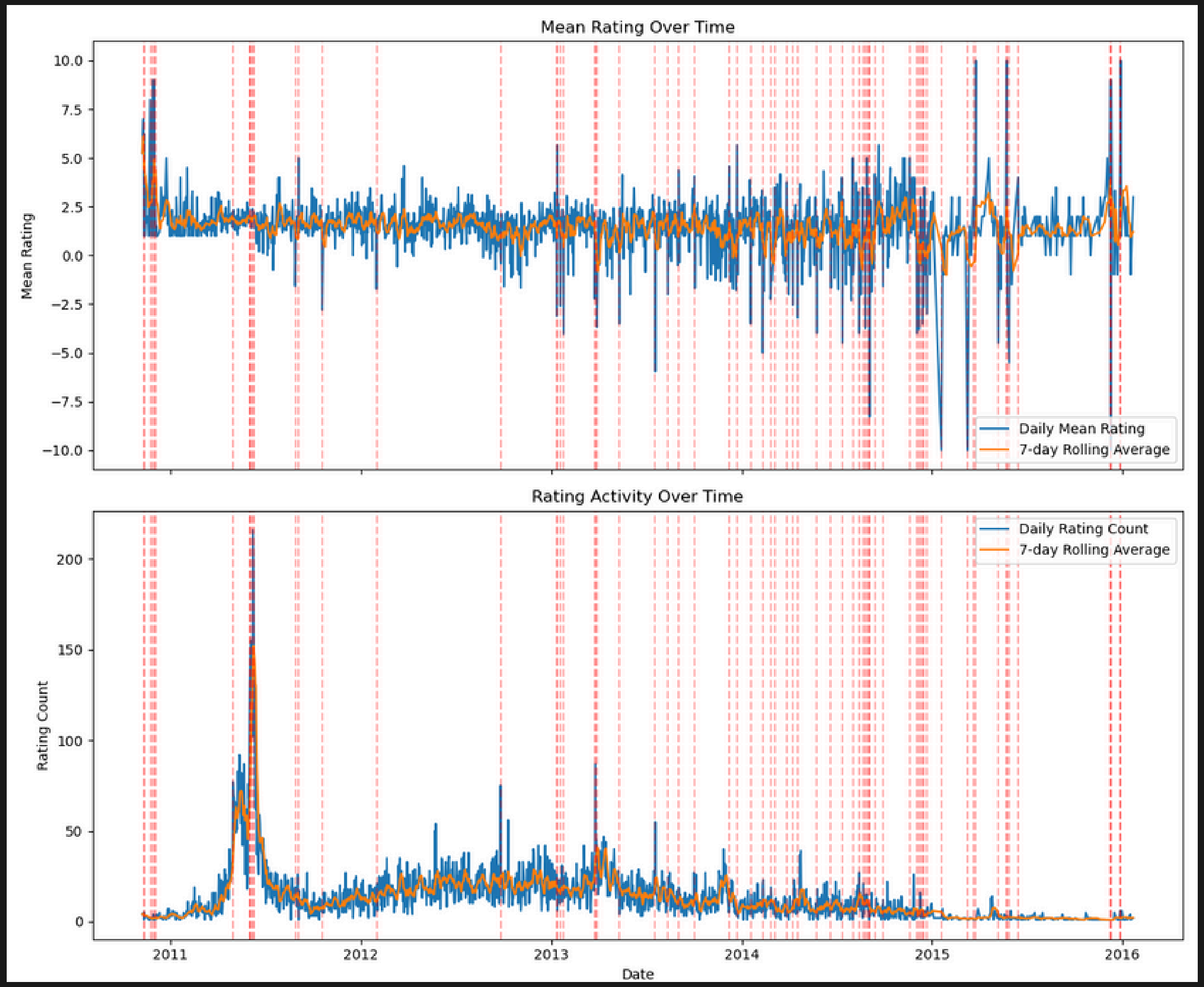
INTUITION

TRUST RATINGS AREN'T STATIC; THEY EVOLVE OVER TIME, INFLUENCED BY MARKET EVENTS, PLATFORM CHANGES, OR COORDINATED ACTIONS. EXTREME FLUCTUATIONS IN RATINGS OVER SHORT PERIODS MIGHT INDICATE SIGNIFICANT EVENTS OR MANIPULATION ATTEMPTS.

FINDINGS

THE ANALYSIS UNCOVERED 71 DAYS WITH STATISTICALLY UNUSUAL RATING PATTERNS BETWEEN 2010 AND 2015. KEY OBSERVATIONS:

- EARLY PLATFORM ACTIVITY (2011): HIGH VARIANCE WITH EXTREME RATINGS.
- PEAK ACTIVITY (2011-2012): HIGHEST RATING VOLUMES WITH STABLE MEANS.
- LATE 2010 ANOMALIES: EXTREME TRUST RATINGS IN LATE NOVEMBER.
- DECEMBER 2015: AN ANOMALOUS DAY WITH AN AVERAGE RATING OF -10. NOTABLY, USERS LIKE ID 7564 (45 RATINGS) AND ID 130 (20 RATINGS) WERE HIGHLY ACTIVE DURING THESE PERIODS, SUGGESTING POTENTIAL INFLUENCE OR COORDINATED BEHAVIOR.



IMPLICATIONS

TEMPORAL ANOMALIES CAN SERVE AS EARLY WARNING SIGNS OF MARKET MANIPULATION OR SIGNIFICANT PLATFORM EVENTS. REAL-TIME MONITORING OF RATING PATTERNS CAN HELP PLATFORMS RESPOND SWIFTLY TO UNUSUAL ACTIVITIES, PROTECTING USERS FROM POTENTIAL FRAUD.

TRUST ASYMMETRY PATTERNS

INTUITION

IN ANY SOCIAL NETWORK, SOME LEVEL OF ASYMMETRY IN RELATIONSHIPS IS EXPECTED—TRUST ISN'T ALWAYS MUTUAL. HOWEVER, EXTREME ASYMMETRIES, WHERE ONE USER TRUSTS ANOTHER HIGHLY WHILE BEING DISTRUSTED IN RETURN, MIGHT INDICATE CONFLICTS, RETALIATORY BEHAVIOR, OR MANIPULATION ATTEMPTS.

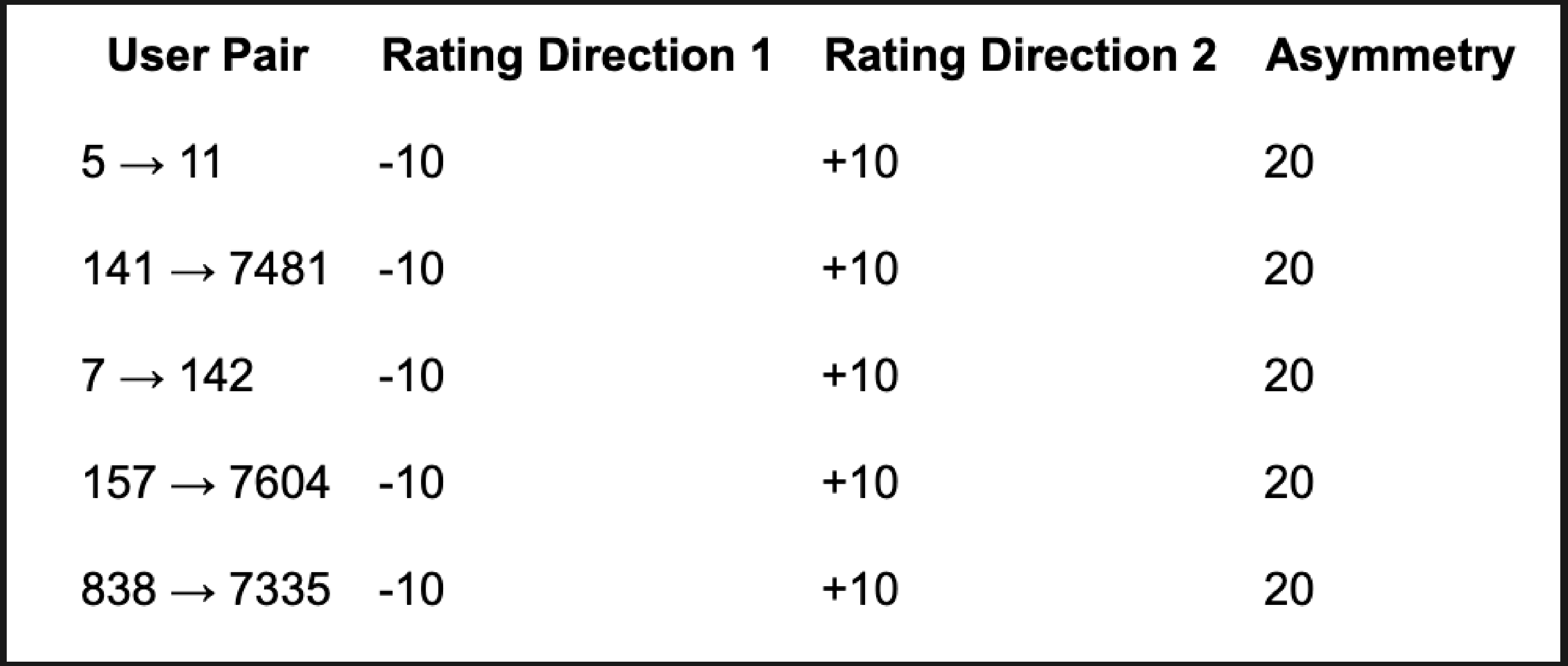
FINDINGS

THE ANALYSIS IDENTIFIED 248 HIGHLY ASYMMETRIC RELATIONSHIPS AMONG 10,062 BIDIRECTIONAL CONNECTIONS. THE MOST EXTREME CASES SHOW MAXIMUM ASYMMETRY (E.G., ONE USER RATES +10, THE OTHER RATES -10). THESE COULD STEM FROM:

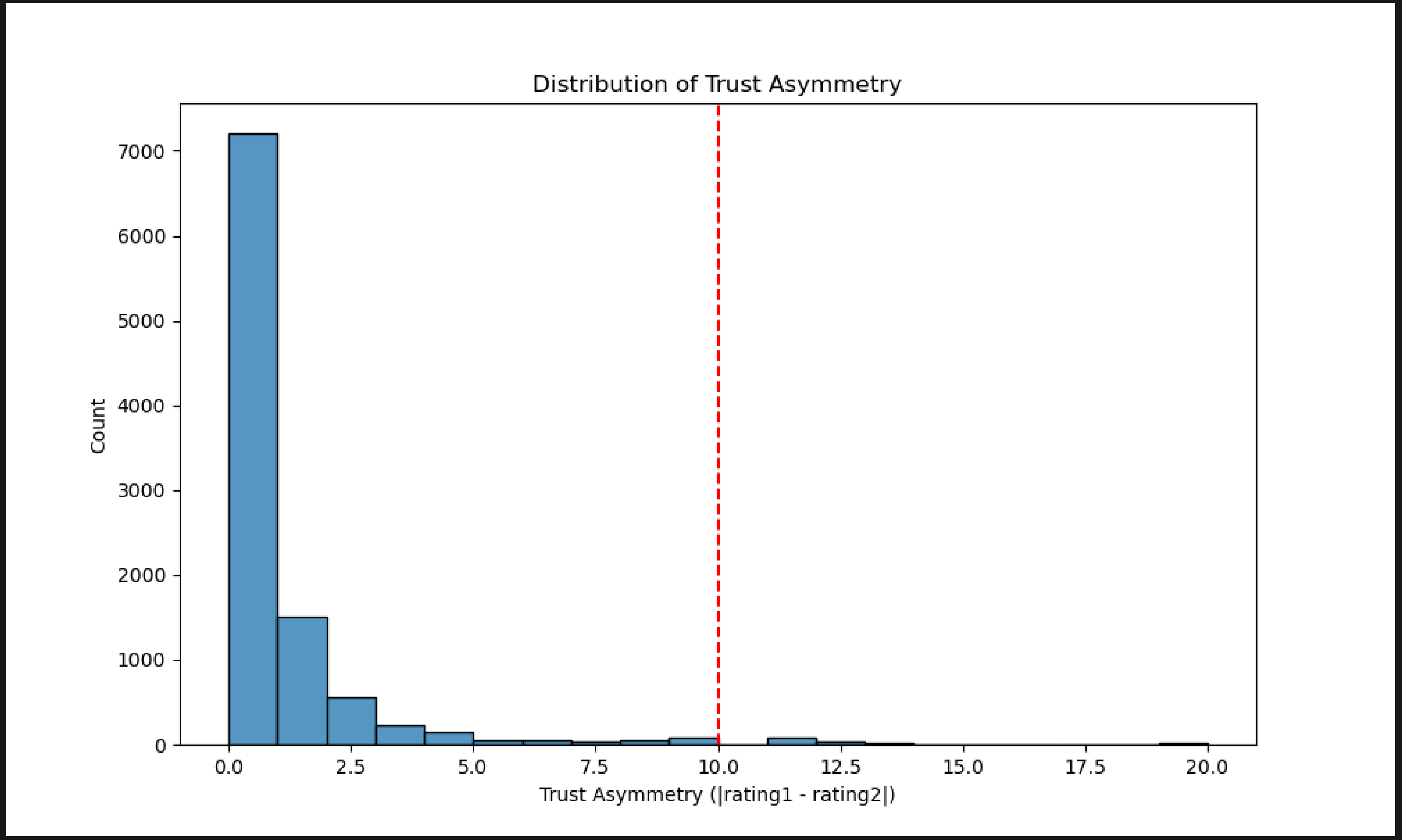
- RETALIATORY RATINGS AFTER DISPUTES.
- ATTEMPTS TO MANIPULATE COMPETITOR REPUTATIONS.
- FUNDAMENTAL DISAGREEMENTS ABOUT TRUSTWORTHINESS.

IMPLICATIONS

SUCH EXTREME ASYMMETRIES CAN DESTABILIZE THE TRUST NETWORK AND MAY REQUIRE INTERVENTION. PLATFORMS SHOULD INVESTIGATE THESE CASES TO UNDERSTAND THE ROOT CAUSES AND PREVENT POTENTIAL ABUSE, ENSURING THE TRUST SYSTEM REMAINS A RELIABLE INDICATOR OF USER REPUTATION.



User Pair	Rating Direction 1	Rating Direction 2	Asymmetry
5 → 11	-10	+10	20
141 → 7481	-10	+10	20
7 → 142	-10	+10	20
157 → 7604	-10	+10	20
838 → 7335	-10	+10	20



NEGATIVE TRUST SUBGRAPHS

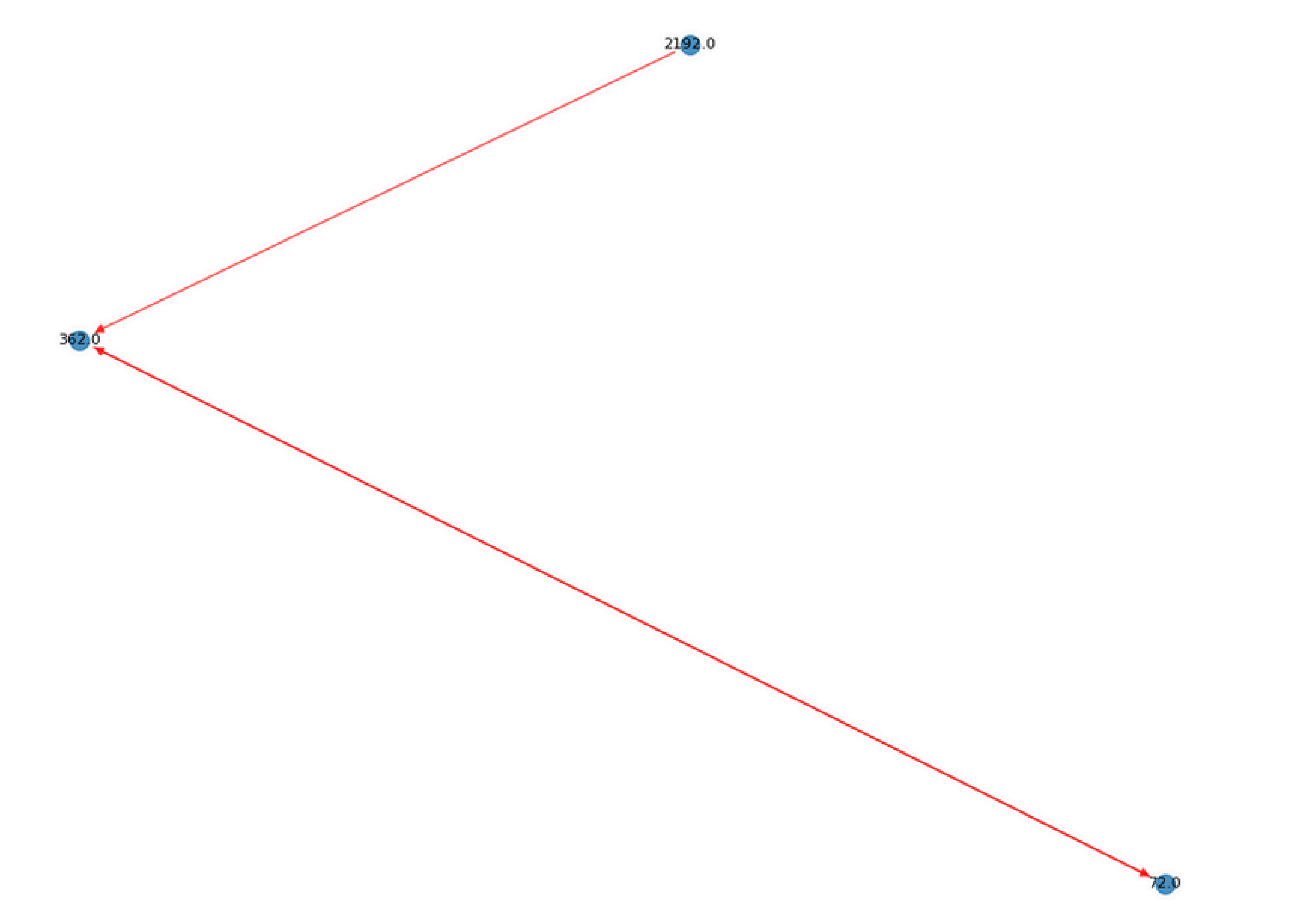
INTUITION

WHILE POSITIVE TRUST IS THE NORM, CLUSTERS OF NEGATIVE TRUST CAN REVEAL POCKETS OF CONFLICT OR DISTRUST WITHIN THE NETWORK. THESE SUBGRAPHS MIGHT REPRESENT COMPETING GROUPS, DISPUTED TRANSACTIONS, OR USERS FLAGGING SCAMMERS.

FINDINGS

HE ANALYSIS FOUND FOUR NOTABLE NEGATIVE TRUST SUBGRAPHS WITH EXCLUSIVELY NEGATIVE CONNECTIONS. THESE CLUSTERS SUGGEST STRONG MUTUAL DISTRUST OR ADVERSARIAL RELATIONSHIPS.

- COMPONENT 1: 3 USERS, ALL NEGATIVE EDGES.
- COMPONENT 2: 3 USERS, ALL NEGATIVE EDGES.
- COMPONENT 4: 4 USERS, ALL NEGATIVE EDGES.
- COMPONENT 6: 4 USERS, 75% NEGATIVE EDGES.



IMPLICATIONS

NEGATIVE TRUST SUBGRAPHS CAN BE HOTSPOTS FOR CONFLICT OR FRAUD. PLATFORMS SHOULD MONITOR THESE AREAS CLOSELY, AS THEY MIGHT INDICATE ONGOING DISPUTES OR COORDINATED ATTACKS ON USER REPUTATIONS. ADDRESSING THESE ISSUES CAN HELP MAINTAIN A HEALTHIER, MORE TRUSTWORTHY ENVIRONMENT.

MANIPULATION RINGS

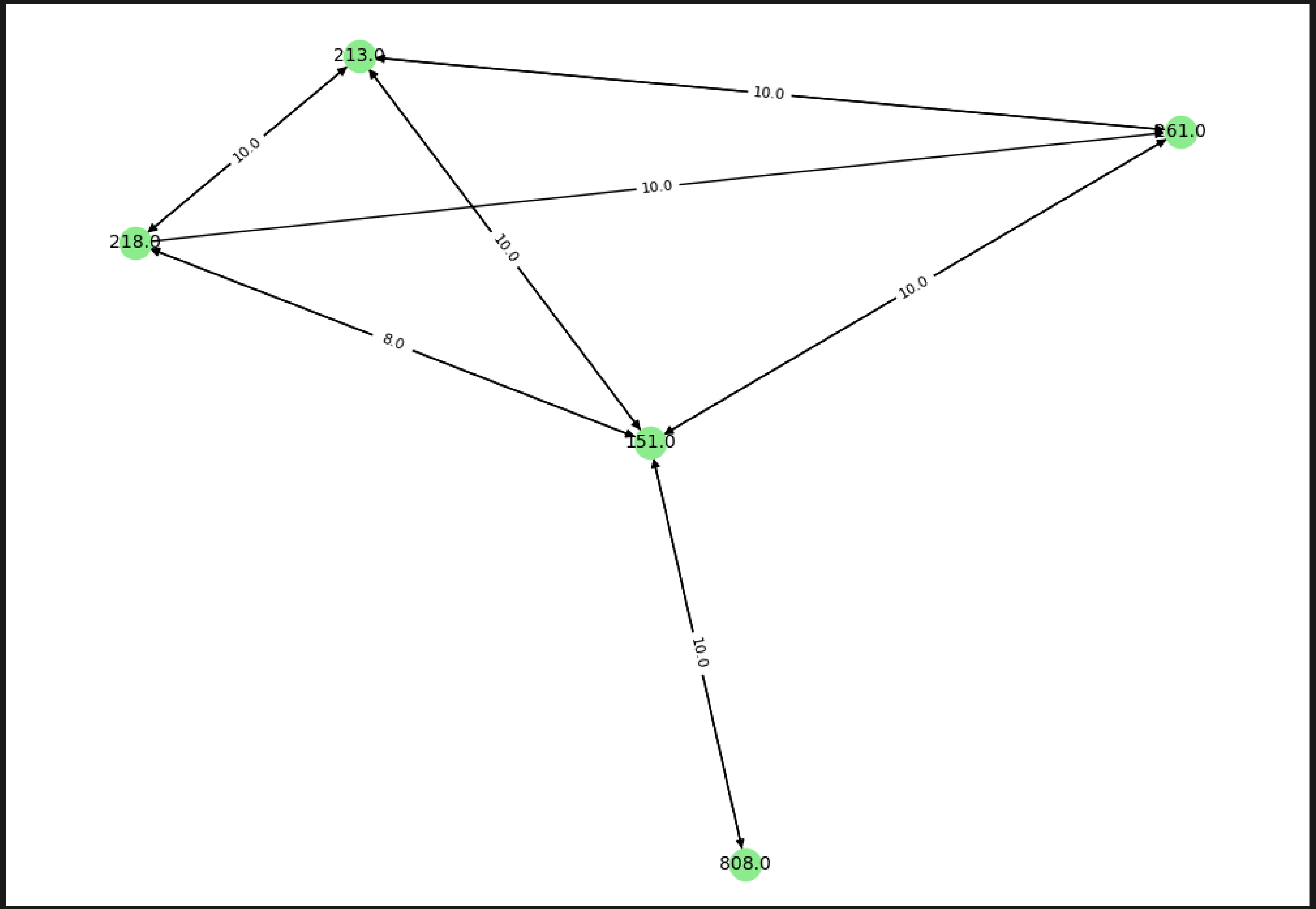
INTUITION

TRUST IS MEANT TO BE EARNED, NOT GAMED. HOWEVER, SOME USERS MIGHT FORM TIGHT-KNIT GROUPS TO ARTIFICIALLY INFLATE EACH OTHER'S TRUST SCORES, CREATING "MANIPULATION RINGS" THAT DISTORT THE PLATFORM'S REPUTATION SYSTEM.

FINDINGS

THE ANALYSIS IDENTIFIED FIVE POTENTIAL MANIPULATION RINGS, SHOWING HIGH INTERNAL TRUST SCORES AND RECIPROCITY, WITH SIGNIFICANT DIFFERENCES FROM EXTERNAL RATINGS.

- COMPONENT 1: 3 USERS, FULLY CONNECTED, AVERAGE RATING OF 10.0, PERFECT RECIPROCITY.
- COMPONENT 2: 5 USERS, DENSITY 0.65, AVERAGE RATING 9.85, HIGH RECIPROCITY.
- COMPONENT 4: 3 USERS, FULLY CONNECTED, AVERAGE RATING 9.17.
- COMPONENT 14: 4 USERS, DENSITY 0.58, AVERAGE RATING 10.0.
- COMPONENT 16: 4 USERS, DENSITY 0.58, AVERAGE RATING 10.0.

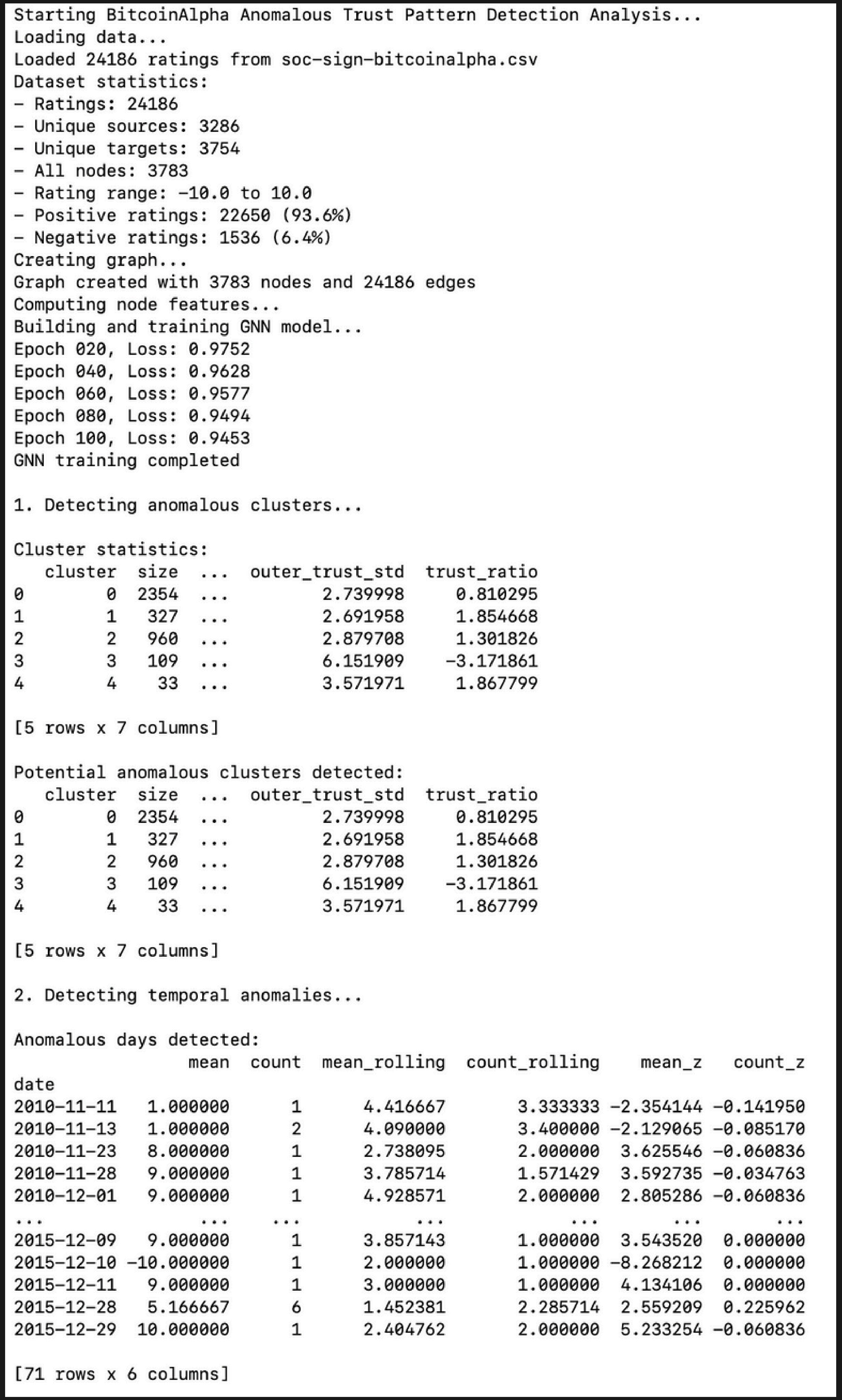


IMPLICATIONS

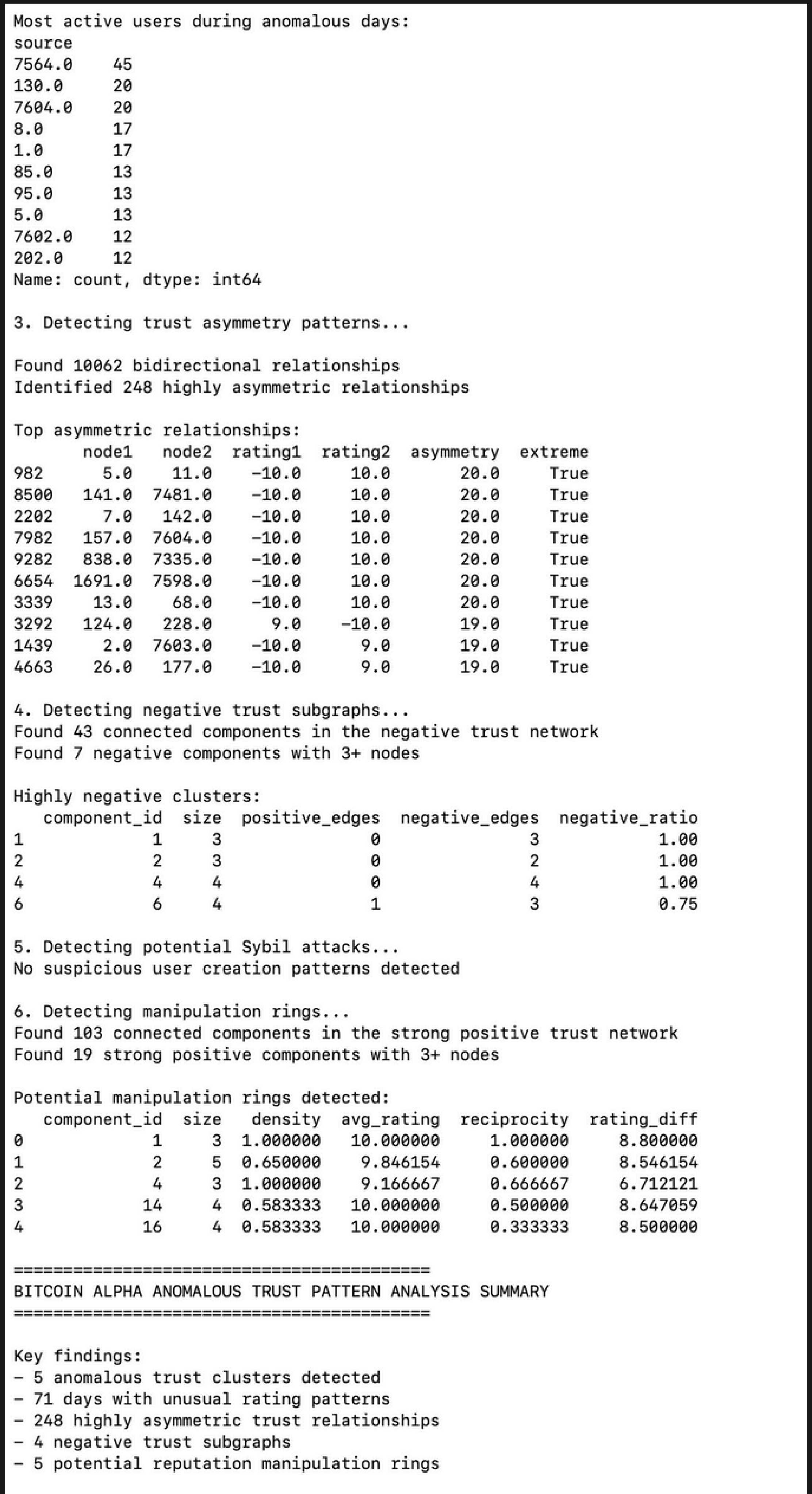
MANIPULATION RINGS CAN ERODE TRUST IN THE PLATFORM'S REPUTATION SYSTEM, LEADING TO FRAUDULENT TRANSACTIONS. PLATFORMS MUST IMPLEMENT DETECTION MECHANISMS TO IDENTIFY & DISMANTLE THESE RINGS, ENSURING THE TRUST NETWORK REFLECTS GENUINE USER INTERACTIONS.

OUTPUT

NOW WE ARE GOING TO PRESENT AN HTML WEBSITE WHICH IS GOING TO HELP YOU VISUALISE THE ANALYSIS DISCUSSED IN THIS DELIVERABLE.



```
Starting BitcoinAlpha Anomalous Trust Pattern Detection Analysis...
Loading data...
Loaded 24186 ratings from soc-sign-bitcoinalpha.csv
Dataset statistics:
- Ratings: 24186
- Unique sources: 3286
- Unique targets: 3754
- All nodes: 3783
- Rating range: -10.0 to 10.0
- Positive ratings: 22650 (93.6%)
- Negative ratings: 1536 (6.4%)
Creating graph...
Graph created with 3783 nodes and 24186 edges
Computing node features...
Building and training GNN model...
Epoch 020, Loss: 0.9752
Epoch 040, Loss: 0.9628
Epoch 060, Loss: 0.9577
Epoch 080, Loss: 0.9494
Epoch 100, Loss: 0.9453
GNN training completed

1. Detecting anomalous clusters...

Cluster statistics:
   cluster  size  ...  outer_trust_std  trust_ratio
0        0  2354  ...         2.739998     0.810295
1        1   327  ...         2.691958     1.854668
2        2   960  ...         2.879708     1.301826
3        3   109  ...         6.151909    -3.171861
4        4    33  ...         3.571971     1.867799

[5 rows x 7 columns]

Potential anomalous clusters detected:
   cluster  size  ...  outer_trust_std  trust_ratio
0        0  2354  ...         2.739998     0.810295
1        1   327  ...         2.691958     1.854668
2        2   960  ...         2.879708     1.301826
3        3   109  ...         6.151909    -3.171861
4        4    33  ...         3.571971     1.867799

[5 rows x 7 columns]

2. Detecting temporal anomalies...

Anomalous days detected:
                 mean  count  mean_rolling  count_rolling    mean_z   count_z
date
2010-11-11   1.000000      1      4.416667       3.333333 -2.354144 -0.141950
2010-11-13   1.000000      2      4.090000       3.400000 -2.129065 -0.085170
2010-11-23   8.000000      1      2.738095       2.000000  3.625546 -0.060836
2010-11-28   9.000000      1      3.785714       1.571429  3.592735 -0.034763
2010-12-01   9.000000      1      4.928571       2.000000  2.805286 -0.060836
...               ...    ...           ...            ...       ...       ...
2015-12-09   9.000000      1      3.857143       1.000000  3.543520  0.000000
2015-12-10 -10.000000      1      2.000000       1.000000 -8.268212  0.000000
2015-12-11   9.000000      1      3.000000       1.000000  4.134106  0.000000
2015-12-28   5.166667      6      1.452381       2.285714  2.559209  0.225962
2015-12-29  10.000000      1      2.404762       2.000000  5.233254 -0.060836

[71 rows x 6 columns]
```



```
Most active users during anomalous days:
source
7564.0    45
130.0     20
7604.0    20
8.0       17
1.0       17
85.0      13
95.0      13
5.0       13
7602.0    12
202.0     12
Name: count, dtype: int64

3. Detecting trust asymmetry patterns...

Found 10062 bidirectional relationships
Identified 248 highly asymmetric relationships

Top asymmetric relationships:
       node1   node2  rating1  rating2  asymmetry  extreme
982      5.0    11.0    -10.0     10.0       20.0     True
8500   141.0  7481.0    -10.0     10.0       20.0     True
2202     7.0   142.0    -10.0     10.0       20.0     True
7982   157.0  7604.0    -10.0     10.0       20.0     True
9282   838.0  7335.0    -10.0     10.0       20.0     True
6654  1691.0  7598.0    -10.0     10.0       20.0     True
3339    13.0    68.0    -10.0     10.0       20.0     True
3292   124.0   228.0      9.0    -10.0       19.0     True
1439     2.0  7603.0    -10.0      9.0       19.0     True
4663    26.0   177.0    -10.0      9.0       19.0     True

4. Detecting negative trust subgraphs...
Found 43 connected components in the negative trust network
Found 7 negative components with 3+ nodes

Highly negative clusters:
   component_id  size  positive_edges  negative_edges  negative_ratio
1             1     3               0               3            1.00
2             2     3               0               2            1.00
4             4     4               0               4            1.00
6             6     4               1               3            0.75

5. Detecting potential Sybil attacks...
No suspicious user creation patterns detected

6. Detecting manipulation rings...
Found 103 connected components in the strong positive trust network
Found 19 strong positive components with 3+ nodes

Potential manipulation rings detected:
   component_id  size   density  avg_rating  reciprocity  rating_diff
0             1     3  1.000000   10.000000     1.000000     8.800000
1             2     5  0.650000    9.846154     0.600000     8.546154
2             4     3  1.000000    9.166667     0.666667     6.712121
3            14     4  0.583333   10.000000     0.500000     8.647059
4            16     4  0.583333   10.000000     0.333333     8.500000

==========================================
BITCOIN ALPHA ANOMALOUS TRUST PATTERN ANALYSIS SUMMARY
==========================================

Key findings:
- 5 anomalous trust clusters detected
- 71 days with unusual rating patterns
- 248 highly asymmetric trust relationships
- 4 negative trust subgraphs
- 5 potential reputation manipulation rings
```

REFERENCES.

DATASET: BITCOIN-ALPHA NETWORK
RESEARCH PAPER: EDGE WEIGTH PREDICTION IN WEIGHTED SIGNED NETWORKS

DELIVERABLE 1: THE DYNAMICS OF EPIDEMIC SPREADING ON SIGNED NETWORKS
DELIVERABLE 2: UNSUPERVISED CLUSTERING OF BITCOIN TRANSACTIONS
DELIVERABLE 3: REV2 - FRAUDULENT USER PREDICTION IN RATING PLATFORMS

THANK YOU.

GROUP 33

RATNANGO GHOSH 2022397

VAIBHAV GUPTA 2022553