Suspicious Activity Detection Using Blockchain Process Mining

B4ISE 25, Vienna

Felipe Alejandro Manzor Manzor, Adam Burke[1], Nagarajan Venkatachalam[1], and **Andrzej Janusz**[1,2]

(1) School of Information Systems, QUT

(2) Centre for Data Science, QUT


Material non-public information (insider trading)
Possible collusion, price fixing
Ordinary market participant
No public price or counterparty trading history
Altered market rules

Audit and transparency mechanisms in traditional markets

- Reduce information asymmetry through price publication
- Disallow disruptive trading patterns
- Detect and prevent fraud & mismanagement
- Anti-money laundering
- Build trust in financial systems

COSO Integrated Framework for implementing controls to prevent, detect, and manage fraud risk related to external financial reporting.

Public blockchains and transparency

- Blockchains offer significantly more public information than traditional exchanges.
- Clear transaction histories do not inherently prevent fraudulent activities.
- Active monitoring and compliance mechanisms are essential.
- Recent High-Profile Cases:
  - FTX Collapse (2022):
  - QuadrigaCX (2019-2022):
  - Crypto "Pump-and-Dump" schemes.

Etherscan

Home | Blockchain | Tokens | NFTs | Resources | Developers | More | Sign In

Top Accounts by ETH Balance ‹/› API

Sponsored: Bitcoin Bull: Raises $100k in Minutes. Hold $BTCBULL, Earn Real $BTC. Could $BTCBULL be Bitcoin's Best Presale?

More than 1,999,999 accounts found (120,725,969.145 ETH)
(Showing the last 10,000 top accounts only)

Download Page Data | First | Page 1 of 400 | Last

#	Address	Name Tag	Balance	Percentage	Txn Count
1	0x00000000...03d7705Fa	Beacon Deposit Contract	61,873,795.80668225 ETH	51.25143848%	665,291
2	0xC02aaA39...83C756Cc2	Wrapped Ether	2,854,132.76793474 ETH	2.36414152%	19,727,878
3	0xBE0eB53F...2404d33E8	Binance 7	1,996,008.36897868 ETH	1.65333804%	2,261
4	0x49048044...fAF74E97e	Base: Base Portal	1,833,336.77872484 ETH	1.51859355%	1,101,936
5	0x40B38765...6e418E489	Robinhood	1,376,694.80331823 ETH	1.14034686%	283
6	0x8315177a...4DBd7ed3a	Arbitrum: Bridge	1,106,089.31658547 ETH	0.91619833%	160
7	0x742d35Cc...e4438f44e	Bitfinex 2	877,645.1461011 ETH	0.72697296%	25,103
8	0x0E58e899...893d9BfCD	Upbit 41	778,046.29657817 ETH	0.64447302%	30,672
9	0x47ac0Fb4...507a6D503	Binance: Binance-Peg Tokens	554,999.05780194 ETH	0.45971804%	448
10	0xE92d1A43...88f85226f	Bitfinex 19	450,118.33054108 ETH	0.37284300%	544

Top 100 Richest Bitcoin Addresses

	Address	Balance	% of coins	First In	Last In	Ins	First Out	Last Out	Outs
1	34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo wallet: Binance-coldwallet	248,598 BTC ($26,897,430,943)	1.25%	2018-10-18 22:59:18	2025-05-14 13:55:53	5413	2018-10-18 23:19:26	2023-01-07 16:15:34	451
2	bc1ql49ydapnjafl5t2cp9zqpjwe6pdgmxy98859v2 wallet: Robinhood-coldwallet	140,575 BTC ($15,209,730,898)	0.7075%	2023-05-09 04:42:20	2025-05-04 11:40:33	453	2023-05-10 09:16:11	2025-01-09 00:54:36	383
3	bc1qgdjqv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjwvw97 wallet: Bitfinex-coldwallet	139,010 BTC ($15,040,430,512)	0.6996%	2019-08-16 20:00:29	2025-04-28 00:07:06	296	2020-02-03 03:43:14	2025-04-23 22:25:30	294

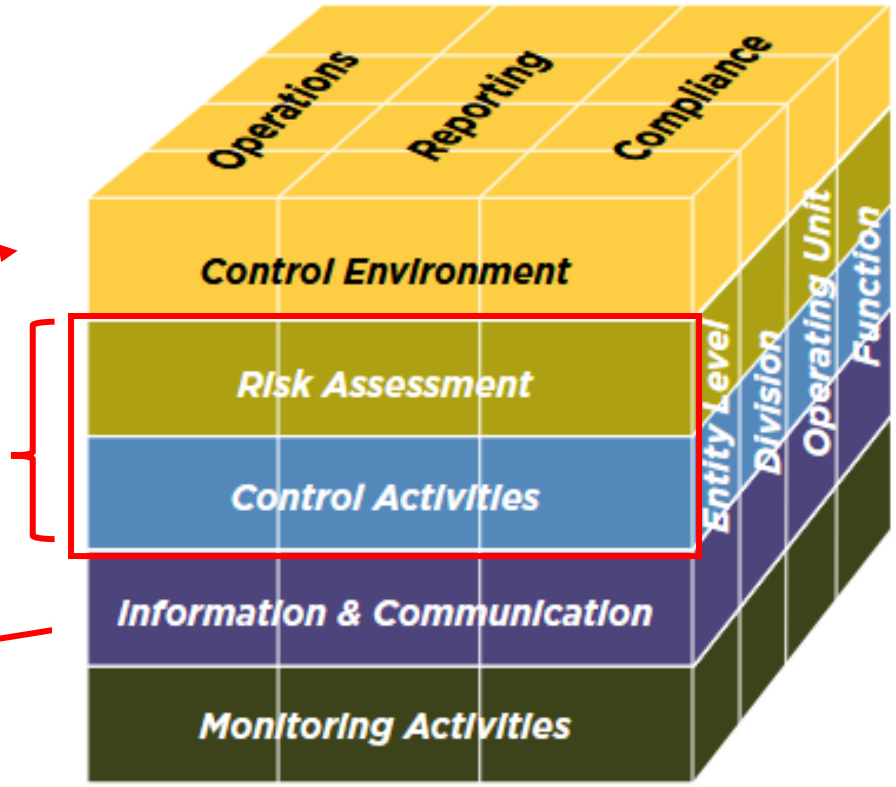
Linking blockchain and forensic audits

This research contributes to practical techniques for analysing blockchain-based systems using **process mining** and **data analytics**, with direct implications for **audit, regulation, and governance** that can also be adapted to different frameworks

Blockchain

Process Mining & Outlier Detection based on smart contracts

Visualization Tools (SN)



COSO Integrated Framework

CryptoKitties game overview

User

Buy

Breed

Gene mix

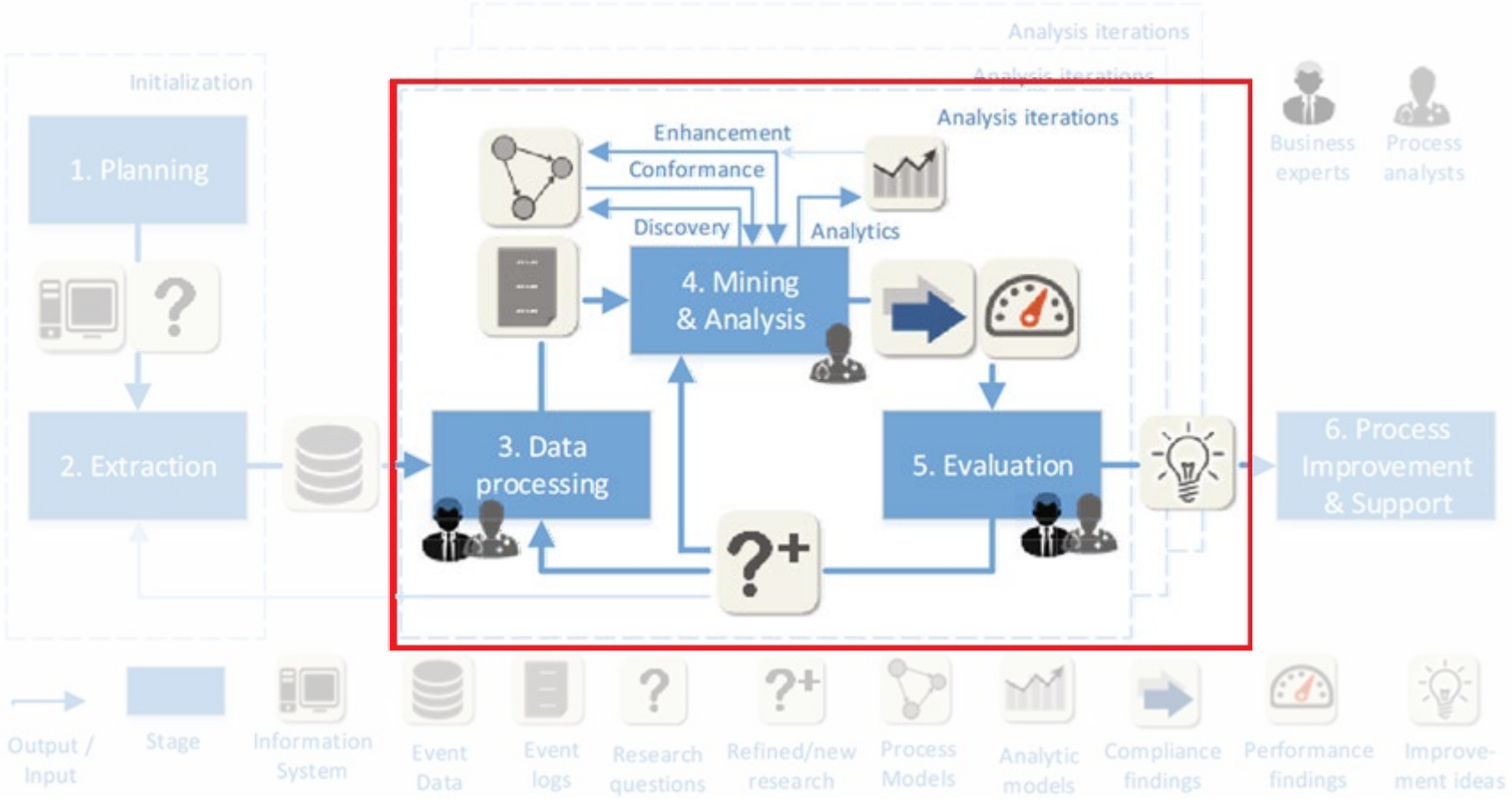
Sell

- Base colour
- Accent colour
- Highlight colour
- Eye colour
- Fur
- Pattern
- Eye shape
- Mouth
- Environment
- Wild
- Prestige
- Secret

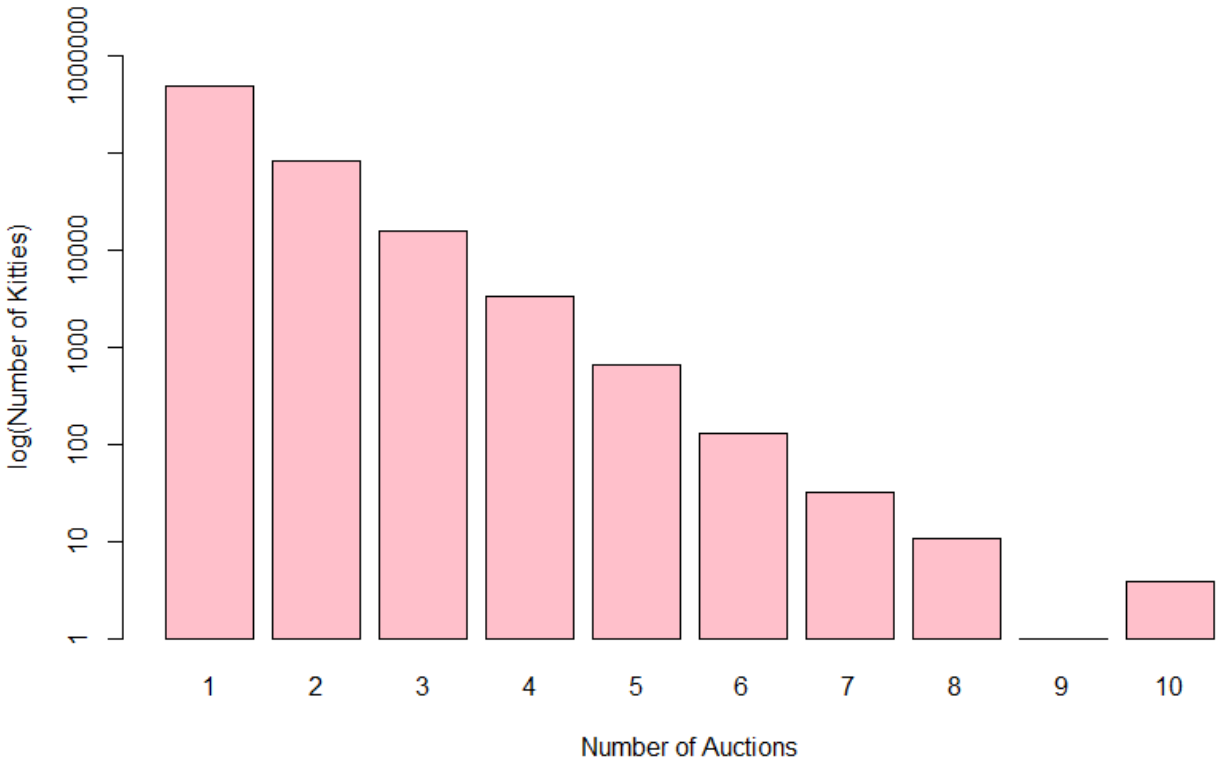
+850M possible combinations

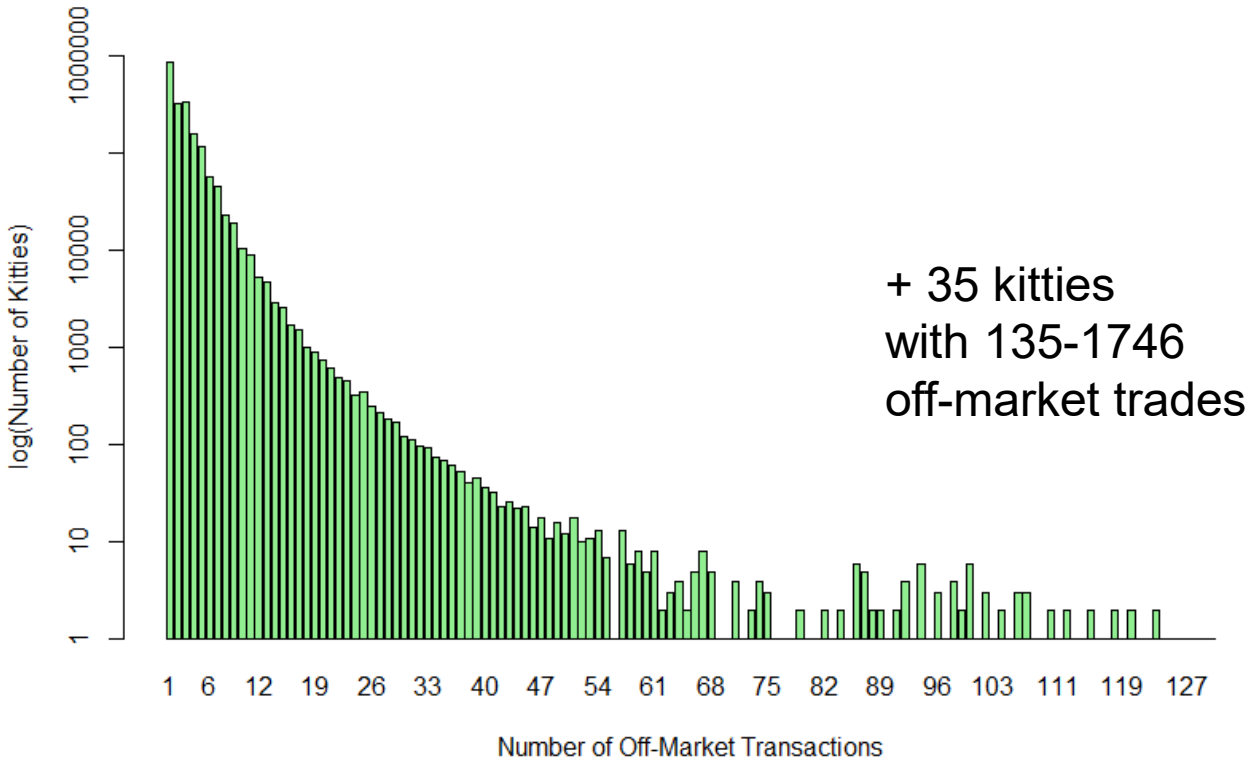
Our methodology

Process mining project methodology (Eck Maikel,2015)



Learning about the data – high-variance activities

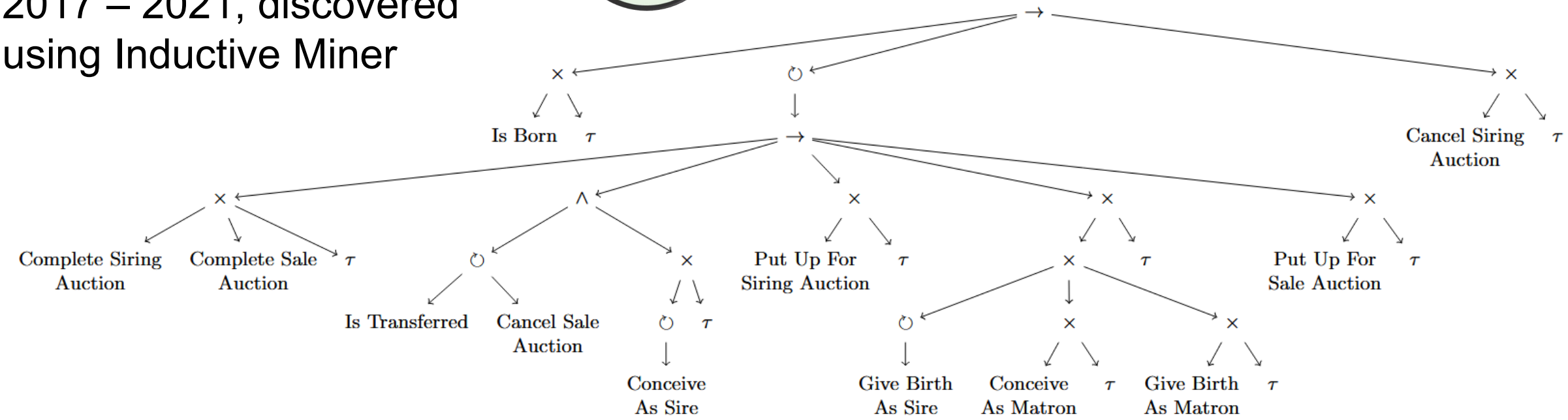




+ 35 kitties
with 135-1746
off-market trades

Learning about the game – process models

Process model tree for genetic clones of LilBub Kitty, 2017 – 2021, discovered using Inductive Miner

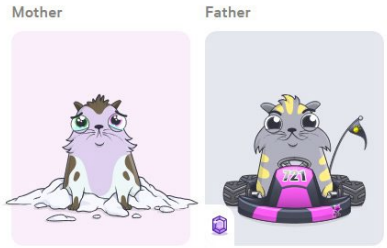


Uneconomic transactions

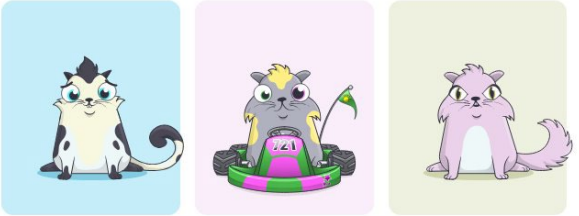
Dioscuri Balinese

https://www.cryptokitties.co/kitty/995907 →
Dioscuri Balinese → Number of transfers = 1,684

Parents



Children

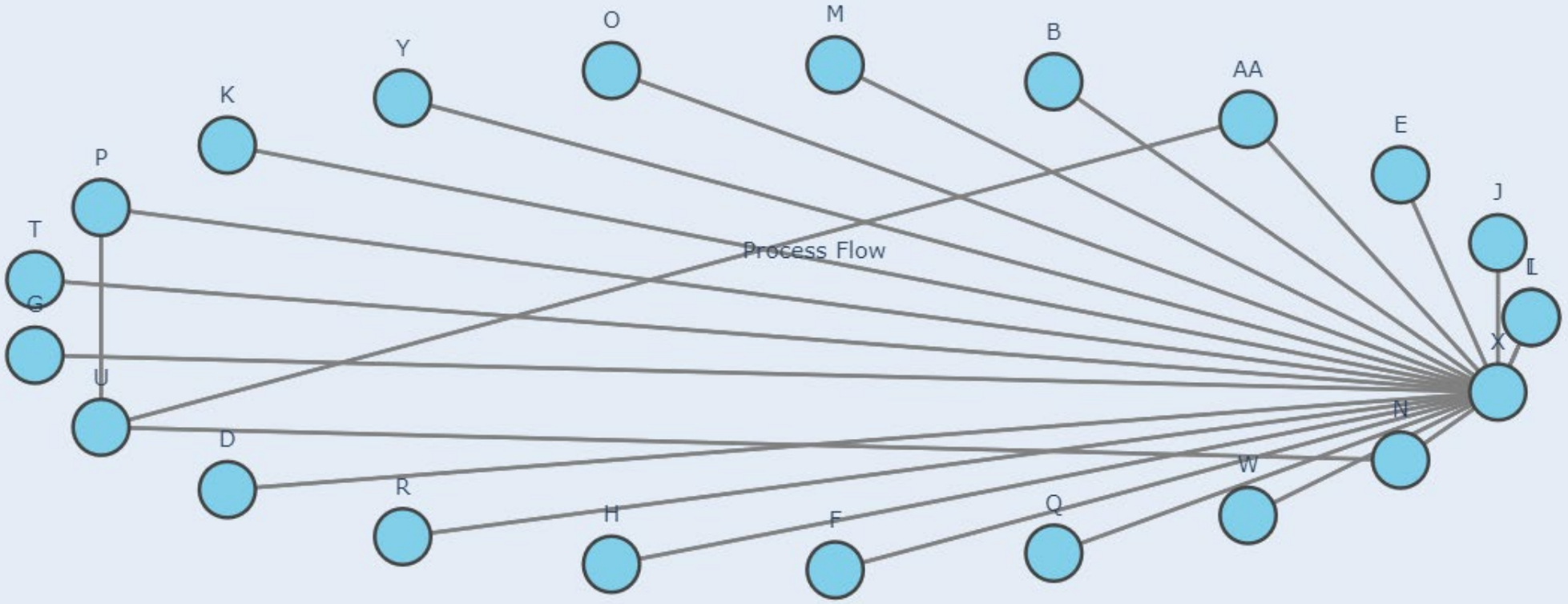


Exemplary transactions involving Dioscuri Balinese:

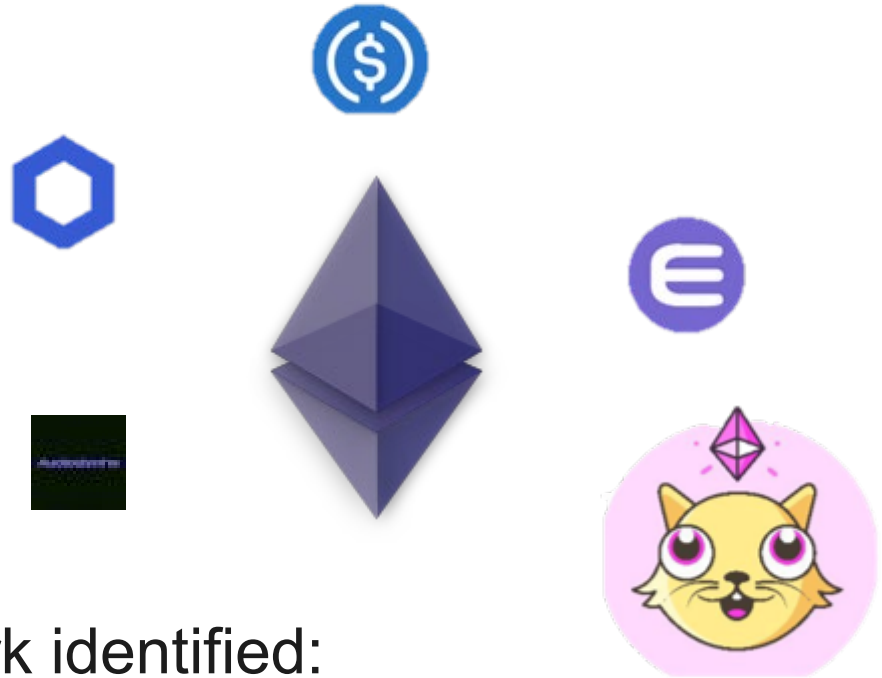
Field	Transaction 1	Transaction 2
Block	7217473	8601703
Time (Local)	14-02-2019	23-09-2019
ETH Price	5.28×10^{-2}	5.55×10^{-2}
ETH Transaction Fee	0.27×10^{-2}	0.46×10^{-2}
Fee Ratio	5.19 %	8.29 %

Social network analysis

Social network graph for transactions involving Dioscuri Balinese Kitty



Key Findings



1. Market rule violations.
   - Duplicate genetics detected.
2. Price manipulation evidence.
3. Collusive trading patterns - tight-knit wallet network identified:
   - Social network analysis revealed a small group of wallets engaged in frequent inter-trading.
   - Centralised transactions.
4. Transparency ≠ Oversight.
5. Auditing potential

Future directions & recommendations

1. Real-time monitoring & alerts
2. Apply the analysis to other DApps on a scale → cross-network analysis.
3. Enrich behavioural heuristics.
4. Integrate On-Chain & Off-Chain using whitelists and blacklists of addresses.
5. Standardised dashboards for transparency.
6. Policy Engagement → Self-regulatory standards for NFT platforms, DeFi systems, and public blockchains.

Related literature (selected)

1. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Das, G.: Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consumer Electronics Magazine 7 (2018) 6–14
2. Hobeck, R., Klinkm¨uller, C., Bandara, H.M.N.D., Weber, I., van der Aalst, W.M.P.: Process mining on blockchain data: A case study of Augur. In: BPM. LNISA (2021) 306–323
3. Leyer, M., ter Hofstede, A.H., Syed, R.: Detecting weasels at work: a theory-driven behavioural process mining approach. In: BPM. (2023) 337–354
4. Smith, M.S.: The spectacular collapse of cryptokitties. IEEE Spectrum 59(9) (2022) 42–47 Publisher: IEEE.

Thanks for your attention!

Any questions?

Acknowledgement:
We would like to thank the **QUT Centre for Data Science** for supporting this research through a travel grant.