# Suspicious Activity Detection Using Blockchain Process Mining

Felipe Alejandro Manzor Manzor (✉) [1], Adam Burke (✉) [2], Nagarajan Venkatachalam [2], and Andrzej Janusz [2]

[1] Frangipani Labs, Brisbane, fmanzor@fen.uchile.cl
[2] School of Information Systems, Queensland University of Technology, Brisbane
{at.burke,venkat.venkatachalam,andrzej.janusz}@qut.edu.au

**Abstract.** This study investigates the use of process mining in conjunction with blockchain data analysis to enhance transparency and detect market anomalies in decentralised applications. Using CryptoKitties as a case study, a game built around Non-Fungible Tokens (NFTs), we analyse transaction data to identify hidden patterns and irregularities indicative of unethical practices, including black-market activity and price manipulation. This highlights gaps in blockchain governance models and how audit supported by process and data analytics can help address them.

**Key words:** blockchain, audit, process mining

## 1 Introduction

In 2008, the entire global financial system experienced enormous upheaval as it became clear that multiple major financial institutions did not have good information on the worth of their own assets and liabilities. Banks failed and lives were upended as this systemic lack of transparency in instruments such as collateral debt obligations suddenly unwound. The radical transparency of blockchain technologies [1] has been promoted as both a technical and institutional solution to these problems [2]. On the other hand, the collapse of the FTX cryptocurrency exchange in 2022, itself causing billions of dollars in lost investments, serves as a stark illustration of ongoing transparency challenges, even when blockchain technology underpins a system.

Blockchains are decentralised digital ledgers which record data (typically transactions) in cryptographically signed immutable blocks linked in a chain [1]. The technology is designed to allow trust in anonymous counterparties without intermediaries, often glossed with the term "trustless". Though cryptocurrencies such as Bitcoin are the most well-known distributed ledgers, more complex and domain-specific decentralised applications (DApps) exist. For instance, vChain [3] is a supply chain–focused blockchain platform that aims to enhance traceability, and efficiency across the stages of production and distribution, minimizing fraud, counterfeiting, and inefficiencies.

Fig. 1: CryptoKitty "Lil-Bub", ID: 1129880.

Process mining [4] analyses event logs from information systems to discover and optimise business processes. By using real data to compute workflows, it allows the comparison of actual processes with expected models. Distinguishing typical and exceptional behaviour makes process mining a powerful tool for financial audit [5].

This paper is a practical investigation on both the potential for abuse in blockchain-based financial trading systems, and the inbuilt transparency required to expose it. It investigates *how blockchain-based process mining can discover patterns of suspicious trading activity in a blockchain-based massively multiplayer trading game*. This novel use of process mining tools in this setting employs them as an auditor or regulator might, not as final proof of disruptive or illegal market activity, but as one form of evidence for this behaviour by a market participant, building a case that could lead to sanction or regulatory penalties. Others have applied process mining to blockchain data [6, 7], but this public analysis of suspicious trading is not usually possible for institutional financial markets, such as the New York Stock Exchange, because a full set of counterparty and individual asset identifiers are available only to regulators, if at all.

The data for this investigation comes from the game CryptoKitties [8]. At the height of its speculative bubble in 2017, CryptoKitties involved significant sums, with virtual cats being sold for over USD$100,000 each [8]. Other online games such as *Fortnite* have annual revenues measured in billions [1].

In the remainder of this paper, we review background material in Section 2 and survey related work on blockchains and process mining in Section 3. Section 4 discusses the dataset and the use of process mining and data science tools. In Section 5 we highlight suspicious transactions found with these techniques. Section 6 concludes.

## 2 Background

*CryptoKitties* CryptoKitties is a non-fungible token (NFT) game first published on the Ethereum blockchain in November 2017. An NFT is a digital asset representing ownership of unique items, from artwork to virtual pets, each with distinct properties that make it non-interchangeable. In CryptoKitties, players collect, breed, and trade digital cats, each with unique genetic attributes, or "genes", which determine appearance, rarity, and value. Breeding two CryptoKitties creates a new Kitty, whose characteristics derive from the genetic combination of its parents, including potential mutations. Each Kitty belongs to a specific generation, affecting its breeding cooldown — a waiting period that

[1] `https://www.statista.com/statistics/1101939/fortnite-annual-revenue`

increases with each breeding cycle. Gene repetition is highly unlikely under normal conditions, however, administrators are allowed to introduce new kittens to the market, such as LilBub, shown in Figure 1. Players can buy and sell CryptoKitties in an in-game marketplace. Off-market trades are also possible. As these transactions are hosted on the Ethereum blockchain, they are publicly visible and secure, yet lack traditional oversight, enabling direct peer-to-peer exchange without regulatory intervention. This open, trustless environment is foundational to the game's appeal and its susceptibility to speculative trading behaviours.

*Market anomalies and suspicious behaviour* Cheating in markets is as old as markets themselves, but in the modern era exchanges and regulators have devised various rules for fair and orderly trading. Markets can exhibit various anomalies, such as collusion, where there are secret agreements among groups or individuals to set prices, avoid forms of competition, or trade in unregulated black markets. Black markets are characterized by features such as under-the-table payments and wide differences in price and asset information available to different participants [9]. Financial markets are also locations where money laundering can occur, that is, proceeds from criminal activity are introduced for use in the regular economy. Non-economic transactions, such as trading at prices far above or below the market, can be symptoms of money-laundering and connections to criminal activity.

*Process Mining* Process mining [4] is a suite of related analytics techniques for understanding organisational behaviour. Within process mining, *process discovery* is an unsupervised learning problem which produces structured process descriptions, *models*, from collections of sequential event data [4]. Process discovery requires three mandatory identifiers in an event: 1) an *activity*, which identify the task being performed; 2) a *case identifier*, such as an order id in online shopping, to group together one execution of a process; and 3) a *timestamp* which indicates sequence. The collections of events recording the process under consideration are termed *event logs*. An example process model is in Figure 2.

Process discovery algorithms are often designed to produce concise process models which have both a straightforward visual interpretation as control-flows, and a data structure with precise formal semantics. In this paper we use Inductive Miner algorithms [10] for their efficiency processing large data sets and formal guarantees, but a large family of discovery algorithms exist, and it is an open area of research.

## 3 Related Work

Related work includes literature on blockchain applications in corporate governance, process mining in auditing, process mining in decentralized applications, and market anomaly detection.

Blockchain platforms were launched with the promise of radical transparency and radical anonymity delivering both improved governance and financial agency. This has been a matter of broad advocacy and debate; examples include research on how immutability can enhance trust within corporations [11] and improving accountability and transparency in corporate decision making [12]. Research has also looked at how specific organisational work patterns with blockchain can minimise uncertainty and build confidence among stakeholders [13].

Existing research demonstrates the feasibility of extracting standard XES (eXtensible Event Stream) process mining event logs from blockchain data, and the challenges of using these data sources [14, 15]. This paper makes use of those tools and public event logs [14]. Process mining in blockchain environments has focused on DApps and demonstrating the feasibility of mapping transaction flows rather than uncovering blockchain-specific patterns. One study [16] developed heuristics for analysing Ethereum transaction logs, revealing high-level structures of DApp usage and transaction complexity.

Process mining techniques have been shown to effectively detect deviations and compliance issues within purchase processes, with an overview and survey in [5]. Similarly, in blockchain-based processes, process mining can identify deviations from expected workflows and flag compliance violations, leveraging the transparent and traceable nature of blockchain transactions. Process mining has also been used to identify patterns of "weasel" behaviour, such as shirking work or taking credit for other's achievements [17, 18]. Here we look at patterns of suspicious trading behaviour, including among possibly colluding traders.

Earlier works on blockchain process mining established its viability with Ethereum DApps like Augur [6] and Forsage [7]. The Augur case study showed that extracting on-chain logs and applying process mining can yield a clear view of how the DApp is used, verifying its design and even detecting unintended behaviors in the smart contract's execution. Forsage pyramid scheme provided evidence that process mining offers valuable insights for smart contract verification and user-behavior analysis a detailed forensic study of Forsage leveraged blockchain's transparency to quantify the scheme's multi-million-dollar gains and losses and to dissect its fraudulent mechanics. Other studies [19] have evaluated process mining's broader utility for transparency and general behavior analysis across Ethereum-based decentralized applications. Against this backdrop, this study takes a different approach by focusing on suspicious activity detection and governance issues in an NFT-based game ecosystem. Rather than emphasizing only process conformance or general transparency, it aims on irregular patterns like black-market collusion and price manipulation (pump-and-dump trading sequences) within CryptoKitties, uncovering evidence of coordinated inflated transactions among a small group of participants.

## 4 Suspicious Behaviour Discovery Techniques

This section we explain the general analysis methodology, the dataset, and the tools and analysis pipeline.

### 4.1 Methodology

The study used an iterative, exploratory analysis approach well-accepted for process mining projects [20]. It is similar to the $PM^2$ method [20], which identifies stages of Planning, Extracting Data, Process Identification, Data Processing, Mining & Analysis, Evaluation, and Process Improvement & Support. Process discovery and analysis happens throughout all the stages after data has been extracted. This paper focuses on the Data Processing, Mining & Analysis stages, with elements of Evaluation. Process Improvement & Support was not part of this project, but would fit the investigation and enforcement activities performed by a market regulator after suspicious behaviour was identified by particular market participants.

Early investigation focused on getting models of typical lifecycle behaviour and sanity checking them against the CryptoKitties smart contract and descriptions of its intended operation. This allowed the investigation of possible exceptions and edge cases. As in an audit, once individual cases of interest were identified, they were cross-checked for patterns of suspicious behaviour.

### 4.2 Cryptokitties Data

Table 1: Properties of the Cryptokitties event log using a `kittyId` case identifier.

(a) Event log properties.

| Item | Value |
|---|---|
| Traces (Kitties) | 1,997,605 |
| Events | 18,059,296 |
| Activities | 12 |
| Start date | 2017-11-23 |
| End date | 2021-04-15 |
| ETH blocks | 2,530,464 |
| Unique Genes | 1,993,863 |

(b) Activity Frequencies.

| Activity | Mean | Stdv |
|---|---|---|
| Cancel Sale Auction | 0.072789 | 0.354156 |
| Cancel Siring Auction | 0.043439 | 0.256977 |
| Complete Sale Auction | 0.259249 | 0.488925 |
| Complete Siring Auction | 0.041854 | 0.326671 |
| Conceive as Matron | 0.591824 | 1.805093 |
| Conceive as Sire | 0.591824 | 1.913482 |
| Give Birth as Matron | 0.593955 | 1.811559 |
| Give Birth as Sire | 0.593955 | 1.920176 |
| Is Born | 0.593955 | 0.510227 |
| Is Transferred | 1.843852 | 1.988901 |
| Put Up for Sale Auction | 0.269602 | 0.619228 |
| Put Up for Siring Auction | 0.100379 | 0.484080 |
| Total | 5.596678 | 7.775904 |

An existing tool was used to extract Ethereum data and convert to an XES file [14]. Transactions spanned a three year period, covering Ethereum blocks `4,605,167` (origin block) to `12,243,999`. In the process mining approach, each kitty (uniquely identified by its `kittyId`) is treated as a case. This dataset is approximately 8 GB in size. Properties of this dataset are summarised in Table 1, including log properties in Table 1a, and activity detail in Table 1b. As

this includes the start of the platform, and the Kitty lifecycles have no defined termination point, the resulting processes should be representative, even though later events will exist for some cases.

Events include a Kitty identifier (`kittyId`), transaction types as activity names, and a timestamp. For CryptoKitties, there are also attributes for details such as gene identifiers, Kitty sire and matron, wallet counterparties, and sale price information. Case identifier, activity identifier, and sequencing attribute are the minimum required inputs for process mining discovery algorithms.

### 4.3 Analysis Pipeline

Data science tools employed were Python [2]. They included the pm4py process mining library and the DASH plot library for social network analysis. Manual exploration of specific blocks and Kitties was done with blockchain browser tools. The Ethereum Explorer [3] was used for general information on the Ethereum blockchain. The CryptoKitties website also provides viewers specific to the game, which were used to understand fine detail of candidate suspicious cases. Social network analysis was also used to understand transactions among multiple counterparties.

## 5 Results and Discussion

In this section we describe how data science analytic tools were used to identify suspicious trading behaviour. Process mining was used to produce models of typical Cryptokitties lifecycles and trading patterns across the entire population, and for selected cohorts such as genetic clones and highly traded assets. Social network analysis helped pinpoint exceptional and suspicious trading and holding patterns for these assets.

### 5.1 Exploratory Process Mining for Asset Lifecycles

The most informative case notion for this data events in the lifecycle of a single Kitty, as identified by the `kittyId`. By defining the `kittyId` as the case identifier, we capture each Kitty's lifecycle events, from its birth as a matron or sire, through transfers, and auctions, and the parenting of other kitties. In the mechanics of the game, Cryptokitties cannot die, so there are no definitively terminal activities.

Figure 2 is a process model representative of typical Kitty lifecycles. It shows birth (Is Born) as an initial activity, though also that this is not the only way a Kitty can be introduced to the system. Kitties can be transferred either through a sale auction or a direct transfer. Over the course of a kitty's lifespan, they are

[2] Scripts are available at `https://github.com/FelipeManzor/CKTransparency`.
[3] `https://eth.tokenview.io`

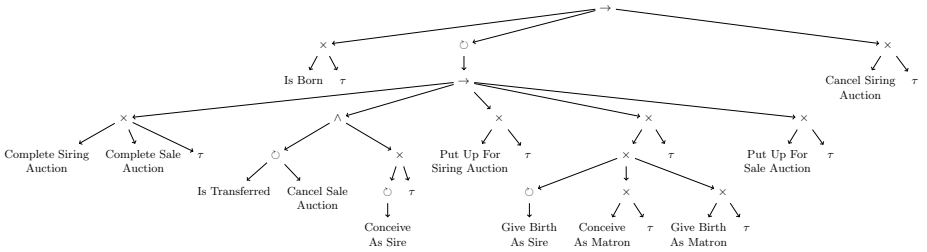


Fig. 2: Process Tree model for Kitties that are genetic clones of "LilBub" (1129880) (see Figure 1), Kitty lifecycle, 2017-2021. Discovered by the Inductive Miner Infrequent (IMf) discovery algorithm.

unlikely to be sold more than eight times. They can also act as a sire or matron, with the right to breed also being tradable through an auction.

Initial exploratory work included generating a process model for the entire Kitty population. For the process discovery step, we employed the Inductive Miner Infrequent (`IMf`) algorithm provided by the `pm4py` library. This choice was motivated by two main considerations. Firstly, Inductive Miner tends to produce well-structured, block-based process models that are relatively straightforward to interpret compared to other discovery algorithms, and is efficient even on very large event logs. Secondly, the infrequent variant (`IMf`) provides a mechanism to ignore highly infrequent paths that may otherwise clutter the model, especially given the extremely large size of our dataset.

Using the Inductive Miner, the full population model showed repeated short loops and concurrency structures symptomatic of fall-through behaviour, which happens when Inductive Miner cannot find other patterns such as sequences or choice. Interestingly, the full-population model also showed the Is Born activity is not the first recorded event for every Kitty. We also explored a case notion of ownership period of a single Kitty for a particular wallet, but it did not generate further insights.

The analysis then turned to population cohorts guided by hypotheses. Three exploratory analysis hypotheses were generated for further exploration.

AH.1 **High variance activities**. An auditor heurisitic is that suspicious activity is more often found in higher variation parts of a process. Activities with high variation in frequency were then considered as a cohort.

AH.2 **Market rules**. Analytic tools allow empirical tests of whether stated market regulatory rules are followed in practice. For CryptoKitties, these are the rules encoded in the smart contract and the game description.

AH.3 **Price manipulation**. Transactions with artificially inflated prices caused by coordinated activities such as pump-and-dump schemes, and their impact on market integrity.

As part of exploring hypothesis AH.1, high variation transaction types are listed in Table 2. Given the size of the dataset and the number of cases, we

Table 2: Deviations

| Activity | Number of Cases | % Over Total |
|---|---|---|
| Is Transferred ( >10) | 34,734 | 1.7% |
| Complete Sale Auction ( >2) | 20,197 | 1.0% |

initially chose a threshold of four standard deviations, expecting it to capture only about 0.01% of all observations, as in a Gaussian distribution. However, our findings show that 1.7% of the cases actually exceed this threshold. The *Transferred* activity represents the change of ownership of a kitty, indicated by a new owner address. *Complete Sale Auction* indicates that the kitty was sold through the CryptoKitties Sales Platform, resulting in a change of ownership.

Standard deviations were also informative when producing the many different process models during this project. A key parameter of the Inductive Miner Infrequent algorithm is the *noise threshold*. We set this threshold based on the standard deviations, ensuring that events or paths occurring below a certain frequency were treated as noise and excluded from the main discovered process model. Given that our dataset comprises more than one million kitties, each with multiple transaction events, the process model could become overly complex if every rare event were included. Consequently, using the infrequent variant of Inductive Miner with a tuned noise threshold allows us to derive generalized models of typical kitty lifecycles, while still highlighting significant outliers in separate analyses. This balanced the need for a high-level process overview and the ability to detect unusual or suspicious transactions that may indicate market manipulation or special-edition assets.

### 5.2 Duplicate Genes

For CryptoKitties, game rules are institutional market rules, the focus for hypothesis AH.2. Though uniqueness is not guaranteed by the platform, as a collectible market, such as for fine art or comic books, the uniqueness of a particular Kitty is part of the value proposition for an owner. The appearance and breeding potential of a Kitty is completely determined by its genetic makeup, and Genetic clones are described by the platform as "responsible for a different trait of a Kitty, and together they combine to make each unique cat [...] there are billions of possible combinations." [4]. Other parts of the documentation emphasise the randomness of breeding and the possibility of mutations.

Each combination of genes is given a unique identifier, `genes`. Using this together with `kittyId` it is straightforward to identify that of the 1,997,605 different kitties in the dataset, there are only 1,993,863 different gene combinations. This leaves 3,742 kitties with duplicated genes, or 0.18%. This high failure rate - over one in a thousand - is arguably inconsistent with the stated rules.

Kitties with the same genetics may also be duplicated may times over. "LilBub" (ID: 1129880), seen in Figure 1, has genetic identifier `1528354362908250337`.

[4] `https://guide.cryptokitties.co/guide/cat-features/cattributes`

136 different kitties possess these genes in this dataset. Figure 2 shows their lifecyles as a process model discovered by Inductive Miner. From analysis of other cohorts, this is quite representative of typical Kitty lifecycles. However, 136 Kitties with identical genetics represent an extraordinary dilution of an expensive collectible asset, akin to buying a baseball card advertised as unique which is then reprinted a hundred times by the vendor. These Kitties also participate in 411 transactions, which is 80 times more than the average number of transactions per Kitty, suggesting scenarios such as high information players selling to lower information market participants who do not realise it is a genetic duplicate.

### 5.3 Market Manipulation

Exploratory hypothesis AH.3 concerns market manipulation. The investigation focused on trading patterns, price, and holding concentration.

Anomalies in CryptoKitties transactions surfaced when analyzing transaction frequency data against established baseline levels, leading to the identification of highly transacted assets. As seen in Table 1b, the mean frequency of the *Is Transferred* activity for each Kitty is 1.84. Kitties traded six times are more than two standard deviations from that mean. Kitties with exceptionally high transaction frequency were identified as anomalies for further investigation. High trading frequencies may simply indicate a popular asset in a deep and liquid market with many participants. However, disparities between market and off-market prices, and transactions at uneconomic prices, often indicate suspicious trading activity.

Among the flagged kitties, one of the most anomalous was the kitty with gene identifier `-3019947904495252141` "Dioscuri Balinese" (kitty ID: `995907`). This kitty registered an extraordinary 1,684 transfers, positioning it far outside the baseline transaction frequency established within four standard deviations of the average. A deeper review using a blockchain explorer revealed that transactions involving this kitty repeatedly occurred at inflated prices, with examples such as `0.055 ETH` and `0.051 ETH`. These trades took place outside the official CryptoKitties marketplace, occurring instead in unregulated environments with little to no oversight. Such settings allow for unmonitored and inflated exchanges, which are characteristic of black-market transactions and indicative of artificial price manipulation. This kitty consistently sold (transferred) off-market at prices substantially exceeding the listed value of `0.0419 ETH`, often approaching nearly ten times the auction price. Only in-game transaction prices are recorded systematically, with off-market prices are not available from a consolidated source. Two representative transactions and spot prices are shown in Table 3. The relatively high transaction costs of 5-8%, multiplied over more than a thousand transactions, is uneconomic, with much more money spent on transaction costs than the underlying value of the asset. Only a single auction (in-game) sale is recorded for this asset.

In addition, only a small number of wallets are involved in trading "Dioscuri Balinese" (ID: 995907). Social network analysis (SNA) reveals this pattern by mapping transaction relationships, where addresses engaged in more than 10

Table 3: Examples of uneconomic transactions from 2019 for Kitty "Dioscuri Balinese" (ID: 995907).

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

transactions with each other are represented as a cohesive network. These transactions are illustrated in Figure 3. The long Ethereum wallet identifiers have been replaced with short alphabetic wallet names for clarity. This figure highlights the structure of potential collusion, which is particularly significant in unregulated markets like CryptoKitties, where demand is difficult to track and validate. In this network, nodes represent addresses, and edges represent frequent transactions between them. Key social network metrics, such as *degree centrality* (indicating how connected an address is) and *betweenness centrality* (highlighting addresses that serve as intermediaries in transaction chains), reveal influential addresses within the network that facilitate these trades. High degree centrality among a few nodes suggests a core group repeatedly trading with each other, reinforcing the hypothesis of a coordinated scheme to inflate perceived demand and value.

Many transactions among a small number of participants would suggest an artificial supply scheme. A small group of wallets maintained ownership until the final transactions, a behavior indicative of market manipulation. As many wallets can be anonymously held by a single person, this may even be the actions of a single trader. The frequent, high-value transfers among select wallets signal coordinated market manipulation efforts, where repeated trades at inflated prices create an illusion of demand and scarcity, typical of black-market strategies. For example, these trades can push up the price of this asset with repeated non-economic sales, before selling it on to another player not in on the scheme.

## 6 Conclusion

In this research, process mining and social network analysis were used to analyse suspicious behaviour in online trading game CryptoKitties. It identified unusual trading, holding and lifecycle patterns, to uncover suspicious behaviour such as possible pump and dump schemes and off-market co-ordination among close groups of participants. Because financial blockchain data makes available counterparty and asset identifiers available only to regulators in markets based on different technologies, even for organisations with extensive market data feeds, we were able to demonstrate suspicious trading behaviours more precisely than otherwise possible on public data or in the existing literature. This suggests that with the right analytic tools, broader market oversight by a wider range

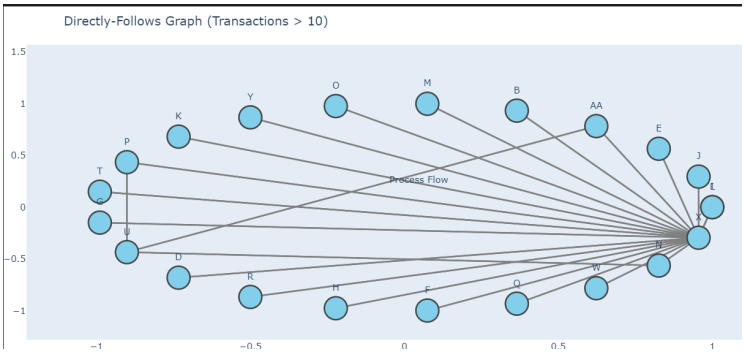


Fig. 3: Wallets with more than ten "Dioscuri Balinese" (ID: 995907) transactions represented as a social network graph.

of organisations is possible with blockchain technology, even while a number of suspicious trading behaviours were discovered in practice. The research also illustrates issues in current governance models by revealing violations of stated market rules.

Genetically duplicate CryptoKitties may not themselves represent a blockchain governance crisis, even though millions of dollars worth of assets were involved at the game's peak, and other games now exist. However, similar certification and trading mechanisms would be involved in, for example, an NFT register for real estate. Not maintaining a one-to-one correspondence between physical asset features and the corresponding ledger certificate would have rather more material consequences when there are duplicated claims for the deed to your family home. The mechanism whereby off-market CryptoKitties transactions could happen at inflated prices not readily accessible to market participants is also representative of governance risks.

One limitation of this study is it does not include validation with the direct CryptoKitties developer and player community, which may have provided alternative explanations and highlighted other interesting analysis hypotheses. We would however also argue that analysing blockchain communities from the perspective of established institutional governance expectations, such as those for orderly trading in financial markets, also contributes to a worthwhile ongoing policy and design discussion.

Overall, this study helps show more concrete ways transparent ledgers can combine with time-aware analytics to surface suspicious behaviour in multi-organisation and adversarial environments. Future work might build new process mining tools and concepts that instrument and extend these capabilities.

## References

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. Sedlmeir, J., Lautenschlager, J., Fridgen, G., Urbach, N.: The transparency challenge of blockchain in organizations. Electronic Markets **32**(3) (September 2022) 1779–1794
3. vChain: About vchain https://www.vchain.io/about . Accessed: 2 Feb. 2025.
4. van der Aalst, W.: Process Mining: Data Science in Action. 2 edn. (2016)
5. Jans, M., Eulerich, M.: Process Mining for Financial Auditing. In: Process Mining Handbook. LNBIP. (2022)
6. Hobeck, R., Klinkmüller, 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
7. Kell, T., Yousaf, H., Allen, S., Meiklejohn, S., Juels, A.: Forsage: Anatomy of a smart-contract pyramid scheme. In: Financial Cryptography and Data Security. Volume 13951 of LNCS. (2024)
8. Smith, M.S.: The spectacular collapse of cryptokitties. IEEE spectrum **59**(9) (2022) 42–47 Publisher: IEEE.
9. Mackaay, E.: Black markets. In: Law and Economics for Civil Law Systems. (2021)
10. Leemans, S.J.J., Fahland, D., van der Aalst, W.M.P.: Scalable process discovery and conformance checking. Software & Systems Modeling **17**(2) (May 2018) 599–631
11. Panisi, F., Buckley, R., Arner, D.W.: Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance? Stanford Journal of Blockchain Law & Policy (2019)
12. Yin, X.: Blockchain Technology in Corporate Governance: Advantages and Limitations. Academic Journal of Business & Management (2023)
13. Müller, M., Ostern, N., Rosemann, M.: Silver bullet for all trust issues? blockchain-based trust patterns for collaborative business processes. In: Business Process Management: Blockchain and Robotic Process Automation Forum. BPM 2020. Volume 393 of LNBIP. (2020) 1–17
14. Klinkmüller, C., Ponomarev, A., Tran, A.B., Weber, I., van der Aalst, W.M.P.: Mining Blockchain Processes: Extracting Process Mining Data from Blockchain Applications. In: Business Process Management: Blockchain and Central and Eastern Europe Forum. BPM 2019. Springer (2019)
15. Moctar-M'Baba, L., Sellami, M., Gaaloul, W., Nanne, M.F.: Blockchain logging for process mining: a systematic review. In: Hawaii International Conference on System Sciences. (2022)
16. Müller, M., Ruppel, P.: Process Mining for Decentralized Applications. In: International Conference on Decentralized Applications and Infrastructures. (2019)
17. Leyer, M., ter Hofstede, A.H., Syed, R.: Detecting weasels at work: a theory-driven behavioural process mining approach. In: BPM. (2023) 337–354
18. Bala, S., Jacobowitz, T., Mendling, J.: Spotting the weasel at work: Mining inappropriate behavior patterns in event logs. In: International Conference on Enterprise Design, Operations, and Computing. (2024) 36–52
19. Hobeck, R., Klinkmüller, C., Bandara, H.M.N.D., Weber, I., van der Aalst, W.: On the suitability of process mining for enhancing transparency of blockchain applications. Business & Information Systems Engineering (2024)
20. van Eck, M., Lu, X., Leemans, S., van der Aalst, W.: $PM^2$: A Process Mining Project Methodology. In: BPM. Volume 9097 of LNISA. (2015) 297–313