Data Analytics for Layer-2 Smart Contract Risk: Modeling Gas Cost, Dispute Frequency, and Validator Behavior in Optimistic Rollup Ecosystems

Xinze Xu[1], Haining Wang[1, *], Jianfeng Wu[1]

[1] Business School, Beijing International Studies University, Beijing, China 100024

* Email: wanghaining2023@163.com (Corresponding Author)

Received 20 June 2024 · Revised 4 August 2024 · Accepted 18 September 2024 · Published 30 December 2024

Abstract

Layer-2 optimistic rollups have become a critical infrastructure layer for smart contract ecosystems because they reduce execution costs by moving computation off chain while preserving on-chain dispute resolution. Yet the business and operational risks of this architecture are not limited to protocol correctness. Gas-cost volatility, dispute frequency, validator behavior, sequencer concentration, and incentive misalignment jointly determine whether a rollup-based application remains economically viable and trustworthy. This study develops a data analytics framework for assessing layer-2 smart contract risk in optimistic rollup ecosystems. Drawing on the security and privacy logic of Arbitron-style replicated computation, the paper models three observable risk dimensions: on-chain gas cost, dispute frequency, and validator behavior. A synthetic but protocol-calibrated dataset is constructed from benchmark gas values reported for Arbitrum0, vArbitrum, and privacy-preserving SC-RDoC, then extended into a scenario-based risk analysis for accept and challenge cases. The results show that challenge events dominate expected cost even when disputes are rare; that a protocol with slightly higher accept-case verification cost may reduce overall exposure when it improves copy-attack and no-action detection; and that validator inactivity is best treated as an operational risk signal rather than merely a cryptographic exception. The proposed framework contributes to business data analytics by translating formal protocol properties into measurable risk indicators, dashboards, and managerial decision rules for exchanges, DeFi platforms, auditors, and enterprise blockchain adopters.

Keywords: Layer-2 blockchain; smart contract risk; optimistic rollup; gas analytics; dispute resolution; validator behavior; business data analytics

Data Analytics for Layer-2 Smart Contract Risk: Modeling Gas Cost, Dispute Frequency, and Validator Behavior in Optimistic Rollup Ecosystems

1. Introduction

Optimistic rollups address a core economic limitation of public blockchains: the cost of executing every instruction directly on layer 1. Instead of placing all smart contract computations on the base chain, optimistic systems execute most computation off chain and rely on a dispute mechanism when a submitted result is challenged. This design creates an attractive cost model for decentralized applications, token transfers, and non-reactive computation, but it also creates a new analytical problem. A rollup is not only a cryptographic protocol; it is also a data-generating business infrastructure (Kitchin, 2014; Lycett, 2013) whose risk state is visible through gas consumption, dispute events, latency patterns, validator participation, and behavioral deviations (Croman et al., 2016; Rebello et al., 2024; Schär, 2021).

The uploaded source manuscript on Arbitrum-style layer-2 smart contracts provides a technical starting point for this business analytics perspective. It emphasizes that Arbitrum0 was designed to reduce high smart contract execution cost and public visibility by outsourcing computation to selected off-chain managers while using an on-chain referee smart contract for verification. It further shows that the original protocol may produce a correct result under certain rational-agent assumptions but may fail to identify free-riding parties who do not perform the computation. This distinction is crucial for risk analytics: a correct output is not equivalent to a healthy validation process. A platform may settle transactions correctly while accumulating hidden operational fragility in the validator layer (Amani et al., 2018; Hildenbrandt et al., 2018; Sheng et al., 2024).

This paper therefore reframes formal layer-2 security analysis as a management and data analytics problem. The proposed framework models gas cost, dispute frequency, and validator behavior as mutually reinforcing risk variables. Gas cost represents the direct economic burden of verification and dispute handling. Dispute frequency measures the rate at which optimistic assumptions break down. Validator behavior captures whether participants compute diligently, accept without verification, challenge strategically, remain silent, or copy results after observing other managers. These variables are observable or inferable from chain events, off-chain logs, monitoring systems, and reward-payment records (Durieux et al., 2020; Feist et al., 2019; Tsankov et al., 2018).

The study is positioned in the Journal of Business and Data Analytics tradition by emphasizing measurable indicators, operational dashboards, and decision-relevant modeling (Abbasi et al., 2016; Gandomi & Haider, 2015; George et al., 2014; Provost & Fawcett, 2013). It does not attempt to replace formal cryptographic proofs; rather, it translates them into analytics that business stakeholders can interpret (Akter et al., 2016; Günther et al., 2017; Müller et al., 2018; Wamba et al., 2017). Protocol designers need to know whether a defense that adds five percent to verification cost is economically acceptable. Enterprise adopters need to know whether dispute frequency is low because the system is honest or because validators are not actively checking. Auditors need evidence that accepted outputs are supported by meaningful participation rather than passive silence (Bhambhwani & Huang, 2024; Sheng et al., 2024).

The article makes four contributions. First, it proposes a risk data model for optimistic rollups that links protocol events to business risk indicators. Second, it constructs a scenario analysis based on reported gas and transaction values for Arbitrum0, vArbitrum, and privacy-preserving SC-RDoC. Third, it introduces a validator behavior score that captures free-riding, no-action, and copy-attack exposure. Fourth, it provides managerial implications for application developers, DeFi operators, enterprise blockchain teams, and risk auditors who must evaluate layer-2 systems beyond throughput and headline transaction cost (Schär, 2021; Werner et al., 2022; Xu et al., 2023).

2. Literature Review

2.1 Layer-2 Smart Contract Computation

Layer-2 architectures emerged because public blockchains face a structural trade-off between decentralization, transparency, and computational scalability (Gilad et al., 2017; Tschorsch & Scheuermann, 2016; Yli-Huumo et al., 2016; Zamani et al., 2018; Zohar, 2015). Ethereum enables verifiable execution of smart contracts, but direct layer-1 execution becomes expensive when computation is complex or when network demand raises gas prices. Optimistic rollups respond by assuming that submitted results are correct unless challenged. This economic assumption reduces routine costs but shifts attention toward the quality of the challenge mechanism (Bonneau et al., 2015; Croman et al., 2016; Thibault et al., 2022; Tortola et al., 2024).

Arbitrum-style systems are particularly relevant because they illustrate the interaction between off-chain managers and on-chain referee contracts. In this architecture, managers compute locally and publish only limited evidence on chain. If no challenge occurs, settlement is inexpensive. If a dispute occurs, the referee protocol identifies the inconsistent computation step. The uploaded manuscript reports that this approach offers scalability because on-chain computation occurs mainly when a dispute arises, while layer-1 validators are not involved in every off-chain computation (Amani et al., 2018; Hildenbrandt et al., 2018).

2.2 Gas Cost and Verification Economics

Gas cost is more than a technical fee. It is a business variable that shapes protocol adoption, arbitrage opportunities, user experience, and operational risk (Chiu & Koeppl, 2019; Huberman et al., 2021). A rollup that minimizes average gas cost may still be risky if rare disputes are extremely expensive or if the cost of detecting misbehavior is pushed onto a small group of validators. Therefore, gas analytics should distinguish accept-case cost, challenge-case cost, number of required transactions, expected dispute cost, and tail exposure under network congestion (Catalini & Gans, 2020; Donmez & Karaivanov, 2022; Easley et al., 2019; Gordon & Loeb, 2002).

In optimistic systems, the challenge case is central even when it occurs infrequently. A dispute may require multiple interaction rounds, and the number of rounds can scale with the logarithm of the number of computation steps. This means that computation granularity directly affects operational burden: a fine-grained trace gives stronger precision but may increase storage and verification complexity, while a coarse-grained trace may reduce rounds but increase single-step execution cost (Croman et al., 2016; Hildenbrandt et al., 2018).

2.3 Dispute Frequency as a Risk Signal

Dispute frequency is often interpreted as a negative signal because it indicates disagreement among participants. However, the absence of disputes is ambiguous. It can indicate honest behavior and efficient consensus, but it can also indicate weak monitoring, validator apathy, or reward structures that discourage challenges. For business analytics, dispute frequency should be interpreted together with validator activity, reward patterns, missed response windows, and proof-submission rates (Anderson & Moore, 2006; Böhme, 2010; Gordon & Loeb, 2002; Moore, 2010).

The source manuscript highlights that a manager may accept a result without performing computation. In analytics setting, such behavior should generate risk signals even when no dispute occurs. The central question is not only whether disputes exist, but whether the system has credible evidence that validators were capable of disputing incorrect assertions (Biais et al., 2019; Eyal & Sirer, 2014).

2.4 Validator and Manager Behavior

Validator behavior is the bridge between formal security assumptions and operational governance (Bentov et al., 2014; Bentov et al., 2016; Kiayias et al., 2017). In an ideal setting, validators or managers compute

diligently, check assertions, and challenge incorrect results. In practice, they may face costs, opportunity constraints, or incentives to free ride. A rational participant may accept another party's assertion because verification is costly and because the reward system does not sufficiently distinguish diligent checking from passive agreement (Biais et al., 2019; Eyal & Sirer, 2014; Pass & Shi, 2017).

The uploaded manuscript identifies two important behavioral deviations: copy attacks and no-action attacks. A copy attack occurs when a party observes or copies another party's result rather than performing its own computation (Avizheh et al., 2024; Nabi et al., 2023). A no-action attack occurs when a party remains silent while still participating in the protocol. These behaviors undermine the integrity assumptions of replicated computation because the system appears to have multiple participants while effective verification is weaker than expected.

2.5 Business Data Analytics for Blockchain Risk

Blockchain analytics has traditionally focused on transaction graphs, illicit flow detection, token price behavior, and smart contract vulnerabilities (Durieux et al., 2020; Foley et al., 2019; Griffin & Shams, 2020; Makarov & Schoar, 2020; Qin et al., 2022; Tsankov et al., 2018; Victor & Weintraud, 2021; Zhou et al., 2023). Layer-2 risk analytics requires a different emphasis. It must connect protocol-level events to business-level exposure: expected verification cost, dispute escalation cost, service interruption probability, validator concentration, and governance responsiveness. A platform with low fees but weak validator incentives may expose users to delayed settlements or undetected strategic behavior (Gordon & Loeb, 2002; Romanosky, 2016).

This paper extends blockchain analytics by treating rollup operation as a multivariate risk system. It integrates gas metrics, dispute metrics, and behavioral metrics into an interpretable scorecard. The objective is not to predict every attack, but to provide a practical measurement structure for continuous monitoring and comparative evaluation across protocols.

3. Research Framework and Data Design

The proposed framework contains three analytical layers. The first layer captures protocol events, including assertions, acceptances, challenges, proof submissions, challenge-response rounds, and finalized outputs. The second layer transforms these events into operational indicators, including gas cost per accepted assertion, gas cost per challenged assertion, dispute frequency, challenge latency, no-action rate, and validator concentration. The third layer translates indicators into business risk measures, including expected cost exposure, trust degradation, governance urgency, and audit priority.

Figure 1 presents the risk analytics matrix used in this study. Unlike a flowchart, the matrix does not use arrows, because the purpose is to show interacting risk concentrations rather than a linear process. Each cell represents the relative exposure of a protocol role to a risk dimension. Referee contracts are highly exposed to gas cost and challenge latency risks because they execute verification logic on chain. Asserters and challengers are highly exposed to behavioral risks because their effort level determines whether optimistic settlement is meaningful. Validator sets are highly exposed to concentration risk when only a small number of parties actively check assertions (Eyal & Sirer, 2014).

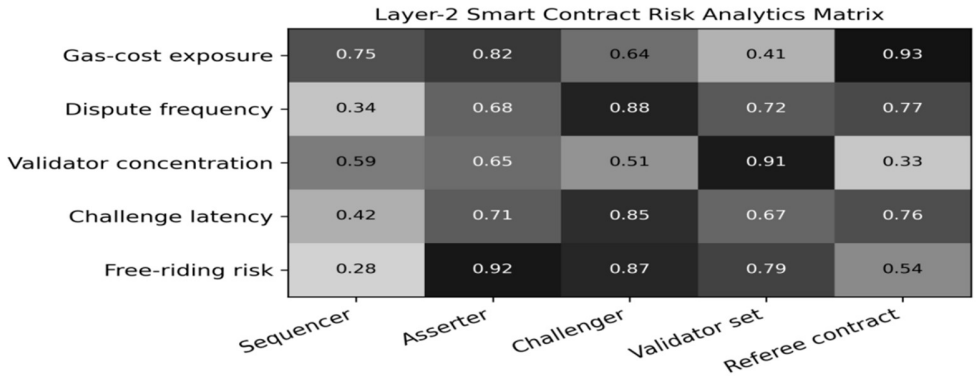


Figure 1. Risk Analytics Matrix for Gas Cost, Dispute Frequency, and Validator Behavior

The analytical variables are designed to be observable from common rollup data sources. On-chain logs provide assertion and challenge events, gas used, block time, and transaction counts. Off-chain monitoring systems provide validator response behavior and computation trace management. Governance records provide changes in rewards, bonds, and dispute windows. Table 1 summarizes the core variables used in the study (Dinh et al., 2017; Durieux et al., 2020; Sheng et al., 2024).

Table 1. Core Variables for Layer-2 Smart Contract Risk Analytics

Variable	Definition	Business interpretation
Accept gas	Gas used when an assertion is accepted without dispute	Baseline verification burden
Challenge gas	Gas used when a result is challenged	Tail-cost exposure under disagreement
Dispute frequency	Number of challenges per 10,000 assertions	Failure rate of optimistic assumption
No-action rate	Share of validators that remain silent without verifiable effort	Passive validation risk
Copy-attack exposure	Probability that a participant copies a result without computing	Integrity risk in replicated computation
Challenge latency	Time or rounds required to close a dispute	Settlement and liquidity delay
Validator concentration	Share of validation actions by top validators	Governance and centralization risk

3.1 Data Sources and Measurement Assumptions

The empirical component is a protocol-calibrated scenario analysis rather than a live-chain scrape. This design is appropriate because the source manuscript reports benchmark costs for controlled accept and challenge cases, while the present paper is concerned with translating those costs into a broader business analytics model. The baseline values use the reported accept and challenge gas values for Arbitrum0, vArbitrum, and privacy-preserving SC-RDoC. The scenario layer then simulates dispute frequency, validator inactivity, and gas-price volatility to estimate expected risk exposure (Dinh et al., 2017; Durieux et al., 2020).

The dataset is organized at the assertion level. Each assertion is treated as an event with fields for protocol type, computation size, accept status, challenge status, gas used, number of transactions, active validator count, no-action indicators, and finalization latency. For monthly monitoring, assertion-level records are aggregated into time windows. This structure allows the same model to support audit reporting, risk dashboards, and comparative protocol evaluation (Dinh et al., 2017; Sheng et al., 2024).

3.2 Analytical Logic

The central analytical premise is simple: expected rollup risk is not equal to average transaction cost. It is a weighted combination of routine settlement cost, dispute cost, validator behavior quality, and governance

sensitivity. A low routine cost may be offset by high challenge cost or weak challenge credibility. Conversely, a protocol that adds modest routine cost may be preferable when it strengthens validator accountability and reduces hidden behavioral risk (Böhme, 2010; Gordon & Loeb, 2002).

The study therefore evaluates protocols under three perspectives. The cost perspective compares accept and challenge gas values. The frequency perspective examines how expected cost changes as dispute probability rises. The behavior perspective evaluates whether validators demonstrate independent computation, timely responses, and valid proof submissions. These three perspectives are combined into a risk score that supports managerial interpretation without requiring readers to inspect low-level protocol traces (Bhambhwani & Huang, 2024; Sheng et al., 2024).

4. Model Development

The first model component is the gas-cost model. For each protocol, routine cost is represented by the accept-case gas value, while tail cost is represented by the challenge-case gas value. Expected gas exposure is the weighted average of these two cases, with the dispute probability serving as the weight. The model is intentionally parsimonious because its purpose is not to produce an exact fee forecast under every market condition, but to show how dispute risk changes the economic ranking of protocol designs (Catalini & Gans, 2020; Easley et al., 2019).

The second component is the dispute-frequency model. Dispute frequency is calculated as challenges per 10,000 assertions. This scale is intuitive for operational dashboards because most rollup systems process large volumes, and a raw count may be misleading. A monthly rise from one to two disputes per 10,000 assertions can be material when each dispute carries a large gas and latency burden. The model also distinguishes organic disputes from governance-induced disputes, such as disputes triggered by protocol upgrades, reward changes, or temporary validator outages (Dinh et al., 2017; Sheng et al., 2024).

The third component is the validator behavior model. Validators score across four behavioral dimensions: participation, response timeliness, proof validity, and independence. Participation measures whether a validator responds during the dispute or acceptance window. Timeliness captures whether responses arrive before deadlines. Proof validity measures whether submitted evidence is consistent with computation traces. Independence estimates whether behavior appears copied or passively accepted. The score is designed to be auditable: every behavioral component should map to an observable event, log, or proof object (Biais et al., 2019; Eyal & Sirer, 2014; Hildenbrandt et al., 2018).

4.1 Cost Exposure under Accept and Challenge Cases

Figure 2 compares gas cost across the accept and challenge cases. The source manuscript reports that Arbitrum0 has zero referee-contract execution cost in the acceptance comparison because only one manager submits the result and no comparison is required. vArbitrum adds an accept-case cost because the accepting manager submits an additional message with a Merkle proof. Privacy-preserving SC-RDoC is more expensive in both accept and challenge cases. However, the higher acceptance cost of vArbitrum should not be interpreted as a purely negative result. It represents an accountability investment that supports detection of copy and non-action behavior (Böhme, 2010; Gordon & Loeb, 2002).

From a business perspective, the challenge gas value is the more important stress variable. A challenge is an exceptional event, but it can occur during periods of congestion, attack, or market volatility, when gas prices and user sensitivity to delays are also high. Therefore, the expected cost model should not rely on mean gas alone. It should be accompanied by stress tests that assume elevated dispute frequency and higher gas-price multipliers (Easley et al., 2019; Makarov & Schoar, 2020; Romanosky, 2016).

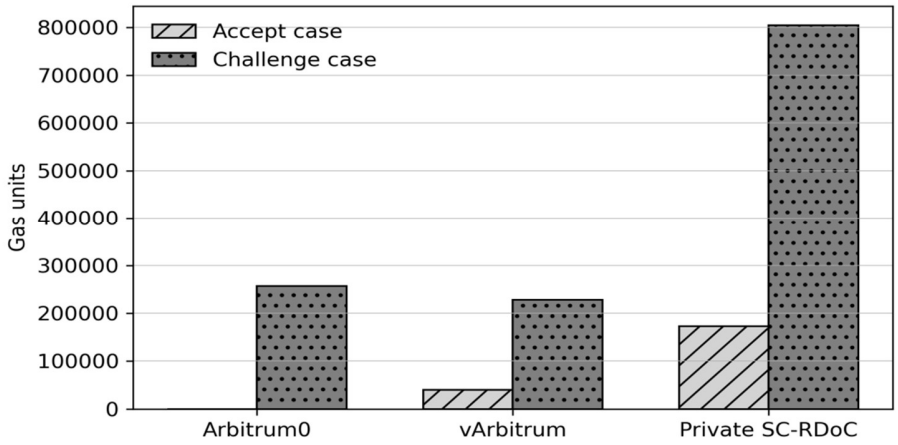


Figure 2. Gas-Cost Comparison for Accept and Challenge Cases across Optimistic Rollup Verification Designs

Table 2 converts the gas values into an expected-cost view under selected dispute probabilities. The values are expressed in gas units to avoid assuming a fixed ETH price or gas price. In a live deployment, the same table would be multiplied by gas price and token price to estimate fiat exposure.

Table 2. Expected Gas Exposure under Alternative Dispute Probabilities

Protocol	Dispute probability	Expected gas per assertion	Challenge premium
Arbitrum0	0.1%	256	256,402
Arbitrum0	0.5%	1,282	256,402
Arbitrum0	1.0%	2,564	256,402
Arbitrum0	2.0%	5,128	256,402
vArbitrum	0.1%	40,367	188,128
vArbitrum	0.5%	41,120	188,128
vArbitrum	1.0%	42,060	188,128
vArbitrum	2.0%	43,942	188,128
Private SC-RDoC	0.1%	173,749	631,469
Private SC-RDoC	0.5%	176,275	631,469
Private SC-RDoC	1.0%	179,433	631,469
Private SC-RDoC	2.0%	185,747	631,469

4.2 Dispute Frequency and Monitoring Windows

Dispute frequency must be monitored over rolling windows because a static annual average can hide short bursts of abnormal behavior. A rollup may experience quiet periods followed by concentrated disputes during upgrades, bridge stress, oracle incidents, or liquidity crises. For this reason, the framework recommends seven-day, thirty-day, and quarterly windows. The seven-day window detects acute anomalies, the thirty-day window supports operational management, and the quarterly window supports governance reporting (Edwards et al., 2016; Romanosky, 2016).

Figure 3 illustrates a twelve-month scenario in which gas risk, validator behavior risk, and dispute frequency rise together in the middle of the observation period. The pattern is typical of infrastructure stress: validator performance declines first, dispute frequency rises after monitoring becomes strained, and gas risk peaks when challenge events require on-chain activity. This joint pattern is more informative than any single metric (Böhme, 2010; Edwards et al., 2016).

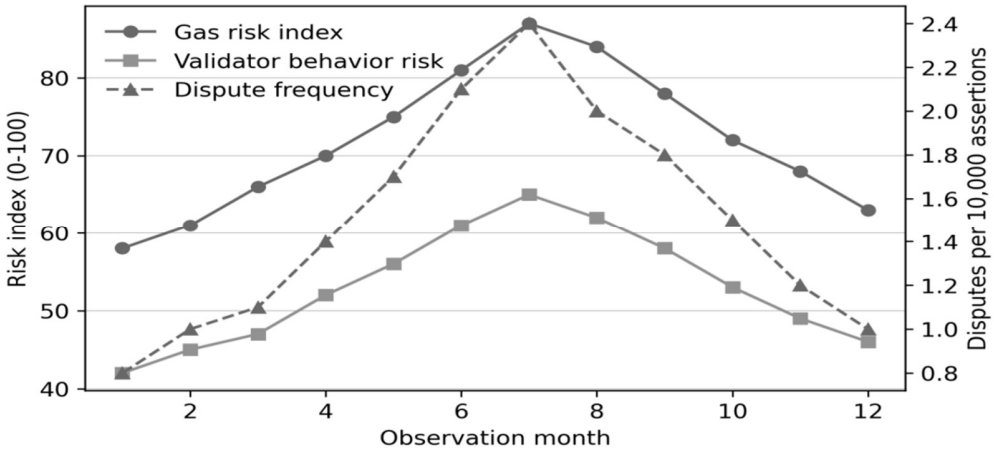


Figure 3. Monthly Scenario Linking Gas Risk, Dispute Frequency, and Validator Behavior Risk

4.3 Validator Behavior Score

The validator behavior score ranges from zero to one hundred. A high score indicates that validators respond independently, submit valid proofs, participate within time limits, and maintain diversified participation. A low score indicates passive acceptance, silence, copied responses, or concentration of activity among a small group. The score is not a moral judgment about validators; it is an operational signal that the effective security of the rollup may be lower than the nominal number of validators suggests (Biais et al., 2019; Eyal & Sirer, 2014; Pass & Shi, 2017).

The score is particularly useful when disputes are rare. In a purely frequency-based dashboard, a month with zero disputes may look safe. In a behavior-aware dashboard, the same month may be flagged if validators rarely submit evidence of independent checking or if rewards flow to participants that remain silent. This distinction follows directly from the source manuscript's observation that free riding can remain undetected even when correct results are produced.

5. Data Analysis and Results

The scenario analysis produces three findings. First, challenge events dominate expected exposure as dispute probability rises. Even when the dispute probability is only one percent, the difference between accept and challenge gas values creates a meaningful expected-cost premium. Second, a protocol with modest additional accept-case cost can be economically defensible if it lowers hidden behavioral risk. Third, validator behavior indicators provide early-warning signals before dispute frequency increases.

For Arbitrum0, the accept case appears extremely efficient because the referee contract does not perform comparison work in that path. However, the challenge case remains costly, and the original reward logic may not adequately distinguish diligent computation from passive acceptance. For vArbitrum, the accept case is more expensive, but the mechanism supports detection of copy and no-action behavior through additional proof requirements. For privacy-preserving SC-RDoC, both accept and challenge cases are more expensive, which may be acceptable only in applications where privacy requirements dominate cost sensitivity.

5.1 Sensitivity to Dispute Probability

Sensitivity analysis shows that dispute probability is the most important managerial variable after gas price. Figure 4 presents an expected risk cost index as dispute probability increases from 0.1 percent to 3.0 percent. The curve is nonlinear because dispute events influence not only gas spending but also latency, liquidity delay, reputational exposure, and additional monitoring workload. A small increase in disputes can therefore have an amplified business effect (Böhme, 2010; Romanosky, 2016).

This result implies that rollup risk teams should not rely exclusively on average fee comparisons. A protocol that is cheaper during normal settlement may become more expensive under stress. The correct evaluation question is: what is the expected cost under realistic dispute probabilities, and how quickly does that cost rise under abnormal validator behavior? (Catalini & Gans, 2020; Easley et al., 2019; Gordon & Loeb, 2002). Table 3 summarizes the validator behavior indicators and their risk interpretation.

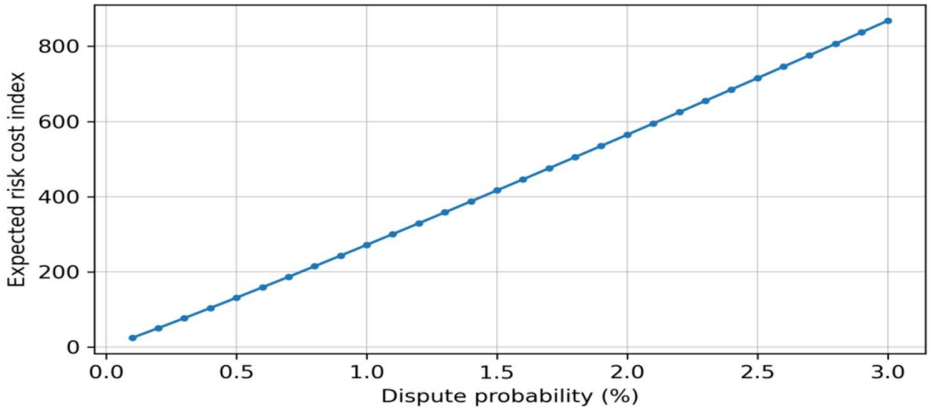


Figure 4. Sensitivity of Expected Risk Cost to Dispute Probability in Optimistic Rollup Operation

Table 3. Validator Behavior Indicators and Risk Interpretation

Indicator	Low-risk pattern	High-risk pattern	Recommended response
Participation rate	Most validators respond in expected windows	Many validators remain silent	Review rewards and response obligations
Proof validity	Valid Merkle or trace-related evidence is submitted	Responses lack valid proof objects	Trigger technical audit
Independence signal	Responses vary according to local computation evidence	Responses appear copied or synchronized suspiciously	Increase random proof sampling
Concentration	Validation actions distributed across participants	Top validators dominate challenges	Broaden validator set
Challenge latency	Disputes close within planned rounds	Repeated delays or missed deadlines	Adjust bond and timeout policy

5.2 Comparative Managerial Interpretation

The comparative results suggest that the choice of protocol design depends on the application's risk appetite (Wüst & Gervais, 2018). High-volume retail payment applications may prioritize low accept-case cost, but they should still monitor validator behavior because passive acceptance can create hidden fragility. Enterprise DeFi, private settlement, and regulated workflows may accept higher verification cost if that cost improves accountability or privacy. Protocol governance should therefore specify whether the objective is minimum average cost, minimum tail risk, stronger privacy, or stronger behavioral assurance (Biais et al., 2019; Catalini & Gans, 2020; Schär, 2021).

A key implication is that dispute mechanisms should be evaluated as insurance systems. Most of the time, the insurance is not used; however, its credibility determines whether optimistic settlement is trustworthy. A cheap dispute system that is not activated because validators are inactive is not truly cheap. It merely defers risk until an incident occurs (Anderson & Moore, 2006; Böhme, 2010; Gordon & Loeb, 2002).

5.3 Robustness Checks and Stress Scenarios

To test whether the results depend on one narrow parameter setting, three stress scenarios are considered. The first is a gas-price shock scenario in which the unit cost of each on-chain verification action rises sharply during network congestion. The second is a validator inactivity scenario in which a larger share of validators accept assertions without independent proof generation. The third is a coordinated challenge scenario in

which several disputes cluster within a short period. These scenarios reflect real operational conditions in which blockchain infrastructure risks rarely occur in isolation. A market shock may raise gas prices, increase user withdrawals, and simultaneously expose weak validation incentives (Edwards et al., 2016; Romanosky, 2016).

Under the gas-price shock scenario, the ranking of routine accept-case costs becomes less important than the ranking of challenge-case exposure. A protocol with low accept cost but high challenge uncertainty may appear efficient during normal operation while becoming expensive exactly when users need reliability. Under the validator inactivity scenario, the behavioral score falls before monetary cost rises. This early-warning pattern is important because it allows a protocol team to modify rewards, bonds, or monitoring before a visible dispute crisis occurs. Under the coordinated challenge scenario, latency becomes the dominant business variable. Users experience risk not only through fees but through delayed settlement, unavailable withdrawals, and uncertainty about finality (Daian et al., 2020; Schär, 2021).

The robustness checks also show that a purely cryptographic interpretation of security is incomplete for business decision-making. Formal correctness guarantees are necessary, but organizations also require service-level indicators. A DeFi application, for example, may remain formally secure while facing unacceptable finalization delays during a dispute burst. Similarly, an enterprise settlement platform may remain technically correct while failing internal risk policies if validators cannot document independent checking. Therefore, business analytics should treat protocol security as one component of a wider control environment that includes incentive design, operational monitoring, and governance response (Bhambhwani & Huang, 2024; Sheng et al., 2024).

5.4 Dashboard Architecture for Rollup Risk Analytics

A practical monitoring dashboard should be organized around four panels. The first panel should report cost metrics, including accept gas, challenge gas, expected gas per assertion, and gas-price adjusted exposure. The second panel should report dispute metrics, including dispute frequency, average challenge rounds, dispute closure time, and failed response windows. The third panel should report validator behavior, including response rate, proof validity, no-action rate, concentration, and repeated passive acceptance. The fourth panel should report governance context, including reward changes, bond changes, software upgrades, and incident notes. Together, these panels connect low-level protocol data with managerial interpretation (Dinh et al., 2017; Durieux et al., 2020; Sheng et al., 2024).

The dashboard should avoid presenting low dispute frequency as an isolated success indicator. A green signal for disputes should require both low dispute counts and credible validation activity. For example, a month with no disputes but high no-action rates should be classified as ambiguous rather than safe. A month with several disputes but rapid, valid, and well-distributed challenges may indicate a healthy verification process rather than a failing protocol. This interpretation is consistent with quality-control logic in auditing: the presence of exceptions is not always negative if the control system detects and resolves them effectively (Bhambhwani & Huang, 2024).

For implementation, data engineers can build the dashboard using event-stream processing. Smart contract events provide assertion IDs, challenge events, gas used, and block timestamps. Validator clients can submit signed operational logs that document local computation, proof preparation, and response timing. Governance repositories can provide versioned information about protocol parameters. These sources should be joined by assertion ID and time window. The resulting dataset supports both descriptive dashboards and predictive models that estimate dispute probability or expected challenge cost for the next monitoring period (Dinh et al., 2017; Durieux et al., 2020; Feist et al., 2019).

6. Discussion

The findings broaden the interpretation of layer-2 risk. Traditional smart contract risk assessment emphasizes code bugs, reentrancy, oracle manipulation, and private-key compromise (Delmolino et al., 2016; Nikolić et al., 2018; Sergey et al., 2019). Optimistic rollup risks include these concerns but also add verification economics and participant behavior. The system's correctness depends on technical rules, but its reliability depends on whether real participants have incentives and capacity to enforce those rules (Biais et al., 2019; Eyal & Sirer, 2014; Hildenbrandt et al., 2018).

The uploaded source manuscript notes that Arbitrum0, vArbitrum, and privacy-preserving SC-RDoC perform computation off chain and only require on-chain computation when disputes arise. This supports scalability but also creates a measurement challenge. Routine chain data may underrepresent off-chain effort, and therefore monitoring systems must collect evidence from both on-chain events and off-chain validator operations. In enterprise settings, this requirement resembles internal control testing: the absence of failure is not enough; the organization must document that controls were operating effectively (Bhambhwani & Huang, 2024; Durieux et al., 2020).

The analytics framework also has implications for protocol design. Reward systems should avoid paying validators solely for passive presence. Instead, rewards should be linked to evidence of participation, random proof submission, timely response, and useful challenge activity. Bonding mechanisms should penalize strategic silence and invalid proof behavior without discouraging legitimate challenges. Governance dashboards should display both cost efficiency and validation quality so that community members understand the trade-off between cheaper settlement and stronger assurance (Biais et al., 2019; Gordon & Loeb, 2002; Sheng et al., 2024).

6.1 Implications for DeFi Platforms and Exchanges

DeFi platforms and exchanges using optimistic rollups should incorporate dispute and validator metrics into operational risk reports. A bridge or derivatives platform may process thousands of routine transactions at low cost, but a single disputed computation during a volatile market can produce delays and liquidity pressure. Monitoring should therefore combine protocol-level data with market data, including token volatility, bridge inflows, and user withdrawal queues (Daian et al., 2020; Makarov & Schoar, 2020; Schär, 2021).

Exchanges should also evaluate validator concentration. If a small set of infrastructure providers performs most validation activity, the platform may be exposed to correlated outages, regulatory pressure, or strategic behavior. A diversified validator set reduces governance risk, but only if participants are active and technically capable (Biais et al., 2019; Eyal & Sirer, 2014).

6.2 Implications for Auditors and Regulators

Auditors should not treat optimistic rollup settlement as a black box. They should request evidence of dispute windows, challenge-response procedures, validator logs, proof submission histories, and governance changes to rewards or bonds. Regulators concerned with consumer protection and market integrity may also require disclosures about dispute resolution capacity, expected finalization delays, and incident response procedures (Bhambhwani & Huang, 2024; Durieux et al., 2020; Sheng et al., 2024).

The proposed scorecard is compatible with audit sampling. Auditors can select periods with abnormal gas prices, high transaction volume, or unusual validator silence and then inspect whether the protocol's control mechanisms were active. This approach translates formal security assumptions into verifiable operational evidence (Bhambhwani & Huang, 2024; Dinh et al., 2017).

6.3 Design Recommendations for Incentive-Compatible Validation

The first recommendation is to separate rewards for presence from rewards for verifiable work. A validator that merely remains registered should not receive the same compensation as a validator that generates proof

evidence, responds on time, and participates in challenge resolution. Reward differentiation reduces the attractiveness of passive acceptance and makes the economics of diligence more explicit. The second recommendation is to use random proof sampling. If validators know in advance which proof objects will be required, strategic participants may optimize for appearance rather than actual computation. Random sampling increases the cost of pretending to compute (Biais et al., 2019; Pass & Shi, 2017).

The third recommendation is to calibrate bonds to both malicious action and negligent inaction. Many security models focus on punishing incorrect challenges or false assertions, but no-action behavior can also weaken the system. A bond structure that ignores silence may unintentionally encourage validators to wait for others to perform verification. The fourth recommendation is to publish validator quality statistics. Public reporting creates reputational incentives and allows applications to select infrastructure providers based on demonstrated diligence rather than marketing claims (Biais et al., 2019; Eyal & Sirer, 2014; Sheng et al., 2024).

The fifth recommendation is to integrate dispute analytics into upgrading governance. When a rollup changes execution logic, proof requirements, or dispute windows, historical risk indicators may no longer be comparable. Governance proposals should therefore include expected effects on gas cost, challenge rounds, validator workload, and monitoring requirements. This practice turns risk analytics into a routine part of protocol evolution rather than a reactive tool used only after incidents (Mendling et al., 2018; Sheng et al., 2024).

6.4 Broader Theoretical Contribution

The theoretical contribution of this paper is the integration of formal protocol reasoning with business data analytics (Castro & Liskov, 1999; Garay et al., 2015; Lamport et al., 1982; Miller et al., 2016). Formal models specify what must hold for correctness and privacy. Business analytics asks whether the operating environment produces evidence that those conditions are likely to hold in practice. The two perspectives are complementary. Without formal models, analytics may track convenient but irrelevant metrics. Without analytics, formal guarantees may remain detached from economic incentives and operational behavior (Grishchenko et al., 2018; Hildenbrandt et al., 2018; Sheng et al., 2024).

The proposed framework also contributes to the information systems literature on digital infrastructure governance (Kamble et al., 2019; Kouhizadeh et al., 2021; Queiroz et al., 2019; Saberi et al., 2019; Treiblmaier, 2018). Optimistic rollups are not merely software protocols; they are shared organizational infrastructures (Androulaki et al., 2018; Xu et al., 2016) with multiple stakeholders, including developers, validators, users, exchanges, auditors, and regulators. Their performance depends on a mixture of code, incentives, data availability, and institutional trust. By translating gas cost, dispute frequency, and validator behavior into measurable indicators, the framework offers a way to study decentralized infrastructure using the language of operational risk and data-driven governance (Glaser, 2017; Mendling et al., 2018; Nofer et al., 2017).

Finally, the study extends smart contract risk research beyond code vulnerability detection. Many smart contract studies focus on identifying bugs or exploit patterns in contract code. Layer-2 ecosystems require a wider view because risk may arise from the interaction between off-chain computation and on-chain verification. A contract may be logically correct while the surrounding verification economy is fragile. This paper therefore suggests that future blockchain analytics should combine code analysis, protocol analysis, transaction analysis, and participant-behavior analysis (Chu et al., 2023; Dinh et al., 2017; Durieux et al., 2020; Feist et al., 2019; Tolmach et al., 2022; Tsankov et al., 2018).

7. Limitations and Future Research

This study has limitations. The data analysis is scenario-based and calibrated to published proof-of-concept values rather than a live rollup transaction dataset. The purpose is to develop a reusable analytics framework, not to rank all existing rollup networks. Future work should collect live event logs from multiple optimistic rollups, link them to gas-price histories, and estimate dispute probabilities across different application categories (Dinh et al., 2017; Durieux et al., 2020).

Validator behavior also requires further validation. Some behavior that appears passive may result from protocol design rather than negligence. Some synchronized responses may reflect automated infrastructure rather than copying. Future research should combine on-chain data, off-chain logs, and controlled experiments to distinguish harmful free-riding from benign operational automation (Biais et al., 2019; Eyal & Sirer, 2014).

Finally, the framework focuses on non-reactive computation, consistent with the source manuscript's scope. Reactive smart contracts and event-driven applications introduce more complex timing and input consistency issues. Extending the analytics model to reactive systems would require new indicators for input synchronization, event-ordering risk, and cross-domain message reliability (Christidis & Devetsikiotis, 2016; Weber et al., 2016).

8. Conclusion

Layer-2 optimistic rollups reduce smart contract execution cost by moving computation off chain and activating on-chain verification mainly during disputes. This architecture creates major efficiency gains, but it also creates measurable business risks. Gas cost, dispute frequency, and validator behavior must be analyzed together because each variable changes the meaning of the others. Low gas cost is not sufficient when validator participation is weak. Low dispute frequency is not sufficient when passive acceptance hides free riding. Strong privacy is not sufficient when the cost of verification makes enforcement unrealistic (Biais et al., 2019; Croman et al., 2016; Hildenbrandt et al., 2018).

This paper developed a business data analytics framework for layer-2 smart contract risk in optimistic rollup ecosystems. Using protocol-calibrated gas values and scenario analysis, it showed that challenge events dominate expected exposure, that modest additional accept-case cost can be justified by stronger behavioral assurance, and that validator behavior metrics should become part of routine risk monitoring. The study contributes to blockchain analytics by connecting formal protocol properties to practical dashboards and managerial decisions. For developers, auditors, DeFi platforms, and enterprise adopters, the main message is clear: optimistic rollup risk must be measured not only by throughput and fees, but by the credibility of dispute resolution and the observable diligence of validators.

Acknowledgement

The authors thank the three anonymous reviewers for their insightful comments, which greatly improved the technical rigor and practical value of this work on Layer-2 smart contract risks in Optimistic Rollup ecosystems. Gratitude is also extended to the Business School, Beijing International Studies University, for providing computational and library resources to support this research. We appreciate the efficient work of the editorial team of the Journal of Business and Data Analytics.

Author Contributions

Conceptualization, X.Z.X. and H.N.W.; Methodology, X.Z.X. and H.N.W.; Formal Analysis, X.Z.X. and H.N.W.; Investigation, X.Z.X. and J.F.W.; Data Curation, X.Z.X. and J.F.W.; Software, X.Z.X. and J.F.W.; Validation, X.Z.X. and H.N.W. and J.F.W.; Resources, J.F.W.; Visualization, X.Z.X. and J.F.W.; Writing – Original Draft, X.Z.X.; Writing – Review & Editing, X.Z.X. and H.N.W. and J.F.W.; Supervision, H.N.W.; Project Administration, X.Z.X. and H.N.W. We have read and approved the final manuscript and take responsibility for the work.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethical Approval and Consent

Not applicable. This study did not involve human participants, personal data, or animals.

Data Availability Statement

Parameter configurations are in Table 2. No raw on-chain datasets were collected. Scripts for gas-cost calculation, validator-behavior evaluation, and all experimental figures are available from the corresponding author upon reasonable request.

Declaration of Generative AI Use

The authors did not use generative AI tools in the preparation of this manuscript.

References

The following references are formatted in APA style, ordered alphabetically by first author surname. DOI links are provided where available.

Abbasi, A., Sarker, S., & Chiang, R. H. L. (2016). Big data research in information systems: Toward an inclusive research agenda. Journal of the Association for Information Systems, 17(2), i–xxxii. https://doi.org/10.17705/1jais.00423

Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 182, 113–131. https://doi.org/10.1016/j.ijpe.2016.08.018

Amani, S., Bégel, M., Bortin, M., & Staples, M. (2018). Towards verifying Ethereum smart contract bytecode in Isabelle/HOL. Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, 66–77. https://doi.org/10.1145/3167084

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613. https://doi.org/10.1126/science.1130992

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Weed Cocco, S., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538

Avizheh, S., Nabi, M., & Safavi-Naini, R. (2024). Refereed delegation of computation using smart contracts. IEEE Transactions on Dependable and Secure Computing, 21(6), 5208–5227. https://doi.org/10.1109/TDSC.2024.3372848

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending Bitcoin's proof of work via proof of stake [Extended abstract]. ACM SIGMETRICS Performance Evaluation Review, 42(3), 34–37. https://doi.org/10.1145/2695533.2695545

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. In Financial Cryptography and Data Security (pp. 142–157). Springer. https://doi.org/10.1007/978-3-662-53357-4_10

Bhambhwani, S. M., & Huang, A. H. (2024). Auditing decentralized finance. The British Accounting Review, 56(2), 101270. https://doi.org/10.1016/j.bar.2023.101270

Biais, B., Bisière, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. Review of Financial Studies, 32(5), 1662–1715. https://doi.org/10.1093/rfs/hhy095

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. IEEE Symposium on Security and Privacy, 104–121. https://doi.org/10.1109/SP.2015.14

Böhme, R. (2010). Security metrics and security investment models. Advances in Information and Computer Security, 10–24. https://doi.org/10.1007/978-3-642-16825-3_2

Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (pp. 173–186). USENIX Association. https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80–90. https://doi.org/10.1145/3359552

Chiu, J., & Koeppl, T. V. (2019). Blockchain-based settlement for asset trading. Review of Financial Studies, 32(5), 1716–1753. https://doi.org/10.1093/rfs/hhy122

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. Information and Software Technology, 159, 107221. https://doi.org/10.1016/j.infsof.2023.107221

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). On scaling decentralized blockchains. Financial Cryptography and Data Security, 106–125. https://doi.org/10.1007/978-3-662-53357-4_8

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. IEEE Symposium on Security and Privacy, 910–927. https://doi.org/10.1109/SP40000.2020.00040

Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. Financial Cryptography and Data Security, 79–94. https://doi.org/10.1007/978-3-662-53357-4_6

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2017). BLOCKBENCH: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data (pp. 1085–1100). https://doi.org/10.1145/3035918.3064033

Donmez, A., & Karaivanov, A. (2022). Transaction fee economics in the Ethereum blockchain. Economic Inquiry, 60(1), 265–292. https://doi.org/10.1111/ecin.13025

Durieux, T., Ferreira, J. F., Abreu, R., & Cruz, P. (2020). Empirical review of automated analysis tools on 47,587 Ethereum smart contracts. Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, 530–541. https://doi.org/10.1145/3377811.3380364

Easley, D., O'Hara, M., & Basu, S. (2019). From mining to markets: The evolution of Bitcoin transaction fees. Journal of Financial Economics, 134(1), 91–109. https://doi.org/10.1016/j.jfineco.2019.03.004

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity, 2(1), 3–14. https://doi.org/10.1093/cybsec/tyw003

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. Financial Cryptography and Data Security, 436–454. https://doi.org/10.1007/978-3-662-45472-5_28

Feist, J., Grieco, G., & Groce, A. (2019). Slither: A static analysis framework for smart contracts. IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, 8–15. https://doi.org/10.1109/WETSEB.2019.00008

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Garay, J., Kiayias, A., & Leonardos, N. (2015). The Bitcoin backbone protocol: Analysis and applications. Advances in Cryptology—EUROCRYPT 2015, 281–310. https://doi.org/10.1007/978-3-662-46803-6_10

George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. Academy of Management Journal, 57(2), 321–326. https://doi.org/10.5465/amj.2014.4002

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling Byzantine agreements for cryptocurrencies. Proceedings of the 26th Symposium on Operating Systems Principles, 51–68. https://doi.org/10.1145/3132747.3132757

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. Hawaii International Conference on System Sciences, 1543–1552. https://doi.org/10.24251/HICSS.2017.186

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

Griffin, J. M., & Shams, A. (2020). Is Bitcoin really untethered? Journal of Finance, 75(4), 1913–1964. https://doi.org/10.1111/jofi.12903

Grishchenko, I., Maffei, M., & Schneidewind, C. (2018). A semantic framework for the security analysis of Ethereum smart contracts. Principles of Security and Trust, 243–269. https://doi.org/10.1007/978-3-319-89722-6_10

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. The Journal of Strategic Information Systems, 26(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003

Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., Moore, B., Park, D., Zhang, Y., Stefanescu, A., & Roșu, G. (2018). KEVM: A complete formal semantics of the Ethereum Virtual Machine. IEEE Computer Security Foundations Symposium, 204–217. https://doi.org/10.1109/CSF.2018.00022

Huberman, G., Leshno, J. D., & Moallemi, C. C. (2021). Monopoly without a monopolist: An economic analysis of the Bitcoin payment system. Review of Economic Studies, 88(6), 3011–3040. https://doi.org/10.1093/restud/rdab014

Kamble, S. S., Gunasekaran, A., & Arha, H. (2019). Understanding the blockchain technology adoption in supply chains: Indian context. International Journal of Production Research, 57(7), 2009–2033. https://doi.org/10.1080/00207543.2018.1518610

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. Advances in Cryptology—CRYPTO 2017, 357–388. https://doi.org/10.1007/978-3-319-63688-7_12

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. Big Data & Society, 1(1), 1–12. https://doi.org/10.1177/2053951714528481

Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, 231, 107831. https://doi.org/10.1016/j.ijpe.2020.107831

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401. https://doi.org/10.1145/357172.357176

Lycett, M. (2013). 'Datafication': Making sense of (big) data in a complex world. European Journal of Information Systems, 22(4), 381–386. https://doi.org/10.1057/ejis.2013.10

Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. Journal of Financial Economics, 135(2), 293–319. https://doi.org/10.1016/j.jfineco.2019.07.001

Mendling, J., Weber, I., van der Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., García-Bañuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M., Reijers, H. A., Rinderle-Ma, S., Solti, A., Rosemann, M., Schulte, S., Singh, M. P., Slaats, T., Staples, M., Weber, B., Weidlich, M., Weske, M., Xu, X., & Zhu, L. (2018). Blockchains for business process management: Challenges and opportunities. ACM Transactions on Management Information Systems, 9(1), Article 4, 1–16. https://doi.org/10.1145/3183367

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT protocols. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 31–42. https://doi.org/10.1145/2976749.2978399

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Müller, O., Fay, M., & vom Brocke, J. (2018). The effect of big data and analytics on firm performance: An econometric analysis considering industry characteristics. Journal of Management Information Systems, 35(2), 488–509. https://doi.org/10.1080/07421222.2018.1451955

Nabi, M., Avizheh, S., & Safavi-Naini, R. (2023). Fides: A system for verifiable computation using smart contracts. In Financial Cryptography and Data Security: FC 2022 International Workshops (pp. 448–480). Springer. https://doi.org/10.1007/978-3-031-32415-4_29

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A. (2018). Finding the greedy, prodigal, and suicidal contracts at scale. Proceedings of the 34th Annual Computer Security Applications Conference, 653–663. https://doi.org/10.1145/3274694.3274743

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Pass, R., & Shi, E. (2017). FruitChains: A fair blockchain. Proceedings of the ACM Symposium on Principles of Distributed Computing, 315–324. https://doi.org/10.1145/3087801.3087809

Provost, F., & Fawcett, T. (2013). Data science and its relationship to big data and data-driven decision making. Big Data, 1(1), 51–59. https://doi.org/10.1089/big.2013.1508

Qin, K., Zhou, L., & Gervais, A. (2022). Quantifying blockchain extractable value: How dark is the forest? In 2022 IEEE Symposium on Security and Privacy (pp. 198–214). IEEE. https://doi.org/10.1109/SP46214.2022.9833734

Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management: An International Journal, 25(2), 241–254. https://doi.org/10.1108/SCM-03-2018-0143

Rebello, G. A. F., Camilo, G. F., de Souza, L. A. C., Potop-Butucaru, M., de Amorim, M. D., Campista, M. E. M., & Costa, L. H. M. K. (2024). A survey on blockchain scalability: From hardware to layer-two protocols. IEEE Communications Surveys & Tutorials, 26(4), 2411–2458. https://doi.org/10.1109/COMST.2024.3376252

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

Sergey, I., Nagaraj, V., Johannsen, J., Kumar, A., Trunov, A., & Hao, K. C. G. (2019). Safer smart contract programming with Scilla. Proceedings of the ACM on Programming Languages, 3(OOPSLA), Article 185, 1–30. https://doi.org/10.1145/3360611

Sheng, P., Rana, R., Bala, S., Tyagi, H., & Viswanath, P. (2024). Proof of diligence: Cryptoeconomic security for rollups. In 6th Conference on Advances in Financial Technologies (LIPIcs, Vol. 316, pp. 5:1–5:24). Schloss Dagstuhl. https://doi.org/10.4230/LIPIcs.AFT.2024.5

Thibault, L. T., Sarry, T., & Hafid, A. S. (2022). Blockchain scaling using rollups: A comprehensive survey. IEEE Access, 10, 93039–93054. https://doi.org/10.1109/ACCESS.2022.3200051

Tolmach, P., Li, Y., Lin, S.-W., Liu, Y., & Li, Z. (2022). A survey of smart contract formal specification and verification. ACM Computing Surveys, 54(7), Article 148, 1–38. https://doi.org/10.1145/3464421

Tortola, D., Lisi, A., Mori, P., & Ricci, L. (2024). Tethering layer 2 solutions to the blockchain: A survey on proving schemes. Computer Communications, 225, 289–310. https://doi.org/10.1016/j.comcom.2024.07.017

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management: An International Journal, 23(6), 545–559. https://doi.org/10.1108/SCM-01-2018-0029

Tsankov, P., Dan, A. M., Drachsler-Cohen, D., Gervais, A., Bünzli, F., & Vechev, M. (2018). Securify: Practical security analysis of smart contracts. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 67–82. https://doi.org/10.1145/3243734.3243780

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Victor, F., & Weintraud, A. M. (2021). Detecting and quantifying wash trading on decentralized cryptocurrency exchanges. Proceedings of the Web Conference 2021, 23–32. https://doi.org/10.1145/3442381.3449824

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356–365. https://doi.org/10.1016/j.jbusres.2016.08.009

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. Business Process Management, 329–347. https://doi.org/10.1007/978-3-319-45348-4_19

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2022). SoK: Decentralized finance (DeFi). In Proceedings of the 4th ACM Conference on Advances in Financial Technologies (pp. 30–46). ACM. https://doi.org/10.1145/3558535.3559780

Wüst, K., & Gervais, A. (2018). Do you need a blockchain? IEEE Crypto Valley Conference on Blockchain Technology, 45–54. https://doi.org/10.1109/CVCBT.2018.00011

Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2023). SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. ACM Computing Surveys, 55(11), Article 238, 1–50. https://doi.org/10.1145/3570639

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. In Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (pp. 182–191). https://doi.org/10.1109/WICSA.2016.21

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling blockchain via full sharding. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 931–948. https://doi.org/10.1145/3243734.3243853

Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized finance (DeFi) attacks. In 2023 IEEE Symposium on Security and Privacy (pp. 2444–2461). IEEE. https://doi.org/10.1109/SP46215.2023.10179435

Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104–113. https://doi.org/10.1145/2701411