Permissioned Blockchain Audit Trails for Government Disbursements: Tamper Resistance and Throughput Evaluation

Carol Kpobie[1], Friday Odihi[2], Deborah Ujeh Osahor[3*], Ifeoma E. Okoli[4]

[1]*Deloitte & Touche LLP, San Jose, United States;* msckpobie@gmail.com

[2]*PINNEL Consulting Nig Ltd, Nigeria;* odihison@gmail.com

[3]*Dotmac Technologies Limited, Nigeria;* osahordeborah@gmail.com

[4]*General Electric, GE Vernova & Healthcare, Nigeria;* Ifeomaokoli47@gmail.com

***Corresponding author:** Deborah Ujeh Osahor, osahordeborah@gmail.com

Abstract

Audit trails for government disbursements must be robust, durable and tamper-proof against alteration by the participants that are constrained by the audit trail. Permissioned distributed ledgers have been suggested as a possible solution, but their efficacy in terms of throughput in a government use-case has yet to be tested: high volume, peaky period-end processing, long retention and a small number of trusted entities. This paper conducts a threat modeling and design analysis exercise to identify the threats to the audit trail, derive security properties from it, and assess whether a specified configuration of Hyperledger Fabric can deliver the required throughput. The five-party network, the chaincode and the synthetic workload are described as a design and were not executed. Estimates of throughput and storage are derived from design specifications using mathematics, with no benchmarks measured. The estimates suggest that endorsement bandwidth is the limiting factor, and a design for per-payment endorsement of 3 out of 5 parties and blocks with 2,000 transactions cannot support the assumed period-end peak rate. Centralized ordering erodes the custody defense. The most convincing reason for using a permissioned trail is distributed custody of evidence, rather than immutability, and the paper concludes with an example reference architecture that separates a high-volume record of payments from a low-volume cryptographic anchor.

Keywords: permissioned blockchain; distributed ledger; audit trail; government payments; tamper-proofing; Hyperledger Fabric; transaction capacity; government transparency

DOI: 10.18091/ijsts.spc1.178

1. Introduction

Audit trail in the context of disbursements is expected to be full-proof and robust enough to withstand tampering by the party being constrained by the audit trail (Okoruwa, 2020). This paper explores whether the concept of permissioned distributed ledger could provide such

properties to satisfy the required throughput of the government's disbursements process. The paper is based on a threat model and design analysis.

1.1 The problem of custody

Audit Trail The audit trail is an evidence and its worth is determined by whether a person, who was not at the scene where the record was generated, could trust it. The basis for such trust lies in the issue of custody and that includes who owns the records, who can make any alterations and who will notice the alteration.

Disbursement by the government is another situation where there is a custody problem. The entity disbursing is normally the same entity whose performance will be judged from the record. This means that a treasury having custody of the accounting ledger is having custody of records showing its disbursing activity. Public payment schemes have this kind of weakness.

1.2 Evaluation gap, stance and scope

The statement that a permissioned ledger enhances custody is reasonable but has not been proven in this context under practical loading. Three gaps are relevant here. First, the references list includes one blockchain audit-trail model (Oshoba, 2020) and no performance measurement result of a permissioned platform, hence the need to prove the claim based on design analysis. Secondly, platform performance and government application have never been examined in tandem.

Thirdly, the security argument is always made informally and the words 'tamper-evident' and 'immutable' are used interchangeably. Section 4.2 highlights the three security properties involved. The practice of security engineering requires a clear model of the adversary prior to control selection (Okoruwa, 2020).

The position of this paper is deflationary. In using a permissioned ledger, disbursement audit's trust assumptions are merely redistributed. This is useful in protecting against an insider working solo in one entity (Akeju, 2018) but offers little protection against a treasury that manages its ordering service. The significant contribution of the ledger is distributed custody of the evidence, not immutability.

The scope of this study is the design of the audit trail, its required security properties, specified evaluation environment and resultant mathematics. No field deployment, test run or performance measurement is reported in this paper.

2. Audit Trails in Government Disbursement

This section outlines the contents of the audit trail in terms of requirements R1 to R6 used in Section 4 and the reason why current custody is institutional (Fadayomi, 2019).

2.1 What the trail must contain

The audit trail of a disbursement is a series of assertions, made by different parties at different points in time, proving that the disbursement was properly authorized, accurate, and delivered. The series of assertions goes from the appropriation/obligation through the invoice and approval all the way to the bank confirmation and reconciliation entries. The audit trail is as good as its weakest link between the systems (Fadayomi, 2019; Dosunmu, 2019).

The connection is the weak point. In case systems are connected by manual reference numbers, batch files or post hoc reconciliations, a dedicated individual will be able to abuse the gaps in recordkeeping. Single-source-of-truth systems are applicable in case the agencies have a common reference (Christen, 2012; Unamma, 2019a).

2.2 Why current custody is institutional

The controls protecting this series are institutional – separation of duties, independent custodianship of documents, and sampling-based external audit. Segregation of duties involves both manual and IT-enabled processes and should be thought out in combination (Kobelsky, 2014). Continuous monitoring is now the norm of external assurance, but it relies on sampling just as traditional auditing did (Vasarhelyi, 2004).

Their vulnerability comes from brittleness under digitization. With a single system holding all the assertions, the segregation of duties can be switched by an administrator to any settings he wants to, and the external auditor sees the sample provided by the system itself. The IT governance policies mitigate this problem somewhat (Fadero, 2018), but they are controlled by the very same administrators that the audit trail is designed to control.

2.3 Requirements

R1 Completeness. All disbursement events are accounted for, including unsuccessful, reversed and canceled events.

R2 Ordering. The order of occurrence is set and verifiable, so that precedence, like obligation prior to invoice, can be determined retrospectively.

R3 Integrity. No recorded event can be changed without being detected.

R4 Availability versus retention. The record is available for the retention period required by law.

R5 Selective reporting. The record is available to the auditor without revealing other records or records not within the authorized set.

R6 Independence of custody. No single party can prevent, change, or suppress a record without being detected by another party.

R6 is the requirement that distributed ledgers should deal with the most. R1-R5 can be fulfilled in traditional ways of various difficulties using append only log, restricted access and reconciliation (Okwesa, 2019; Ashcroft, 2002).

2.4 The reporting burden and the volume profile

The peak-to-mean ratio is the crucial parameter from the operational point of view, as the system designed on the mean would fail during the last business days of the period (Aifuwa, 2020; Gama, 2014).

The design workload assumes an example annual volume of 186 million payments, i.e., 15.5 million monthly, or an average volume of 26 tps during 250 eight-hour working days of a year. A fiscal year end peak of 900 tps represents 35 times more than this mean volume. This volume is not measured but is just assumed (Section 5.3).

It is the peak-to-mean ratio that shows if a ledger throughput is enough or not. The design meeting the mean may not meet the requirement in several working days when obligations would accumulate.

3. Distributed Ledger Technology for Permissioned Settings

This section describes a family of platforms evaluated, the consensus and ordering problem, and what the benchmarking literature doesn't show (Eyetsemitan, 2020).

3.1 Platform landscape, 2016–2020

Two platform families are reviewed. Hyperledger Fabric partitions the network into organizations where endorsing peers belong. The transaction is simulated and endorsed by policy-defined peers, ordered by an ordering service and validated and committed by all peers. For this reason, the design of the endorsement policy plays a role in determining throughput.

Corda confines validation of a transaction to the transaction participants, which is better suited for bilateral disbursement rather than a single disbursement log. This paper does not review Corda. The selection of Fabric is driven by a scoping decision rather than its superior capabilities. Permissioned audit trail designs have been suggested (Oshoba, 2020), and this paper adheres to this paradigm.

3.2 Consensus, ordering and benchmark evidence

The ordering service in Fabric is pluggable. Crash fault tolerance ordering, such as Raft ordering provided in the specified configuration, can tolerate the failure of some orderers but cannot tolerate malicious orderers. Byzantine fault tolerance ordering is tolerant to malicious orderers at a cost of increased latency and messaging overhead.

In either case, ordering is performed by a participant that should be constrained by the trail. The trust profile depends on ordering operator identity. In the specified topology, all three orderers

are operated by the treasury organization. Treasury operating the orderers can censor or re-order transactions regardless of the consensus protocol used, unless ordering is witnessed by an independent domain (Eyetsemitan, 2020; Ujkani, 2019).

There is no published performance benchmark of Hyperledger Fabric or any other permissioned platform in the reference list, hence the throughput inputs of Section 6 are assumptions. Published performance benchmarks use simple key-value workloads with small payloads, and therefore, for disbursement chaincode, they are taken as upper bounds, and the reduction factor is an assumption.

Benchmarks also evaluate steady-state throughput, whereas disbursal systems need to meet peak demands that occur in spikes (Gama, 2014). This work bridges that gap through design-level mathematics as opposed to evaluation, a well-known approach in the continuous audit literature (Kogan, 2014).

4. Threat Model and Security Properties

The adversary model identifies five adversarial parties, states tamper-resistance and derives the guarantees which can be achieved by a permissioned ledger. It conforms to security engineering practices by first modelling adversarial threats and then identifying suitable countermeasures (Okoruwa, 2020; Akeju, 2018).

4.1 Adversaries

A1, The disbursing agency alone. The agency seeks to hide or change the record of a payment transaction it undertook. A ledger that has more than one independent replica renders any divergence apparent. Property achieved: strong.

A2, The treasury or central disbursing entity. The treasury runs the payment service and ordering service too, and therefore it can censor transactions. The ledger would help only if there is an independent ordering witness. Property achieved: contingent, often none at all.

A3, The banking intermediary. The bank can falsify its record of receipt or redirect a transaction. Consistently recorded fake receipts remain fake regardless. Property achieved: weak, non-repudiation of the bank's record alone.

A4, The systems administrator. The administrator with database access can modify the rows and set timestamps. This is the attacker where the ledger is most resistant, unless he controls a majority of replicas. Property gained: strong, contingent on the replication architecture.

A5, The external attacker. The external attacker may attempt to modify or inject the record. Authentication is the defense against this attacker, as well as legacy systems. Property gained: moderate, an hygiene improvement.

The strengths of the ledger are focused on A1 and A4, both of which are attacks from inside the same organization (Akeju, 2018; Kranacher, 2011).

4.2 What tamper resistance means

Immutability is the property whereby a record cannot be changed. No deployed distributed system offers it, since administrators can change the storage.

Tamper-evident property is where the change in the record can be detected by the party that verifies it. It is provided through cryptographic chaining within the replica, assuming someone verifies the record (Power, 2013).

Tamper resistance is defined as the property by which no coalition smaller than a certain stated size can make an undetectable change. The blockchain ledger can offer this property and the rest of the paper will analyze it. The three properties are usually confused when making security arguments for permissioned chains.

4.3 Formal statement

Let the trail be a sequence of blocks $B_1, \ldots, B_n$, where each B_i contains a set of transactions and a header $h_i = (H(B_{i-1}), \tau_i, \mu_i)$ with H a collision-resistant hash, τ_i a timestamp, and μ_i a commitment to the block's contents. Let there be m participants, of which f may be adversarial (Okoruwa, 2020).

Definition (tamper resistance). The trail is $((f, \epsilon))$-tamper-resistant if, for any coalition C with $|C| \leq f$, and any alteration α to the trail, the probability that α remains undetected by at least one honest participant's verification procedure is at most ϵ.

Three observations follow immediately.

First, tamper resistance is achieved by replication with independent verification, not by chaining alone. Chaining gives evidence within a replica; the threshold comes from requiring an alteration to be applied consistently to more than f replicas (Mbonu, 2020b).

Secondly, the important threshold is not number of nodes, but a majority of independent administrative domains (Mohammed, 2017; Dosunmu, 2019).

Third, ϵ is not zero. Verification can be defeated by hash collisions, by compromise of the verification software and by attacks on timestamping that change ordering without changing contents. A claim that $\epsilon = 0$ cannot be supported (Okwesa, 2019; Mbonu, 2020).

4.4 Derived properties and their limits

P1, Cross-organizational detectability. With $m \geq 3$ independent administrative domains and $f = 1$, alteration by any single domain is detectable by the others, provided each domain verifies the chain independently. This holds for A1 and A4 and is the ledger's principal contribution.

P2, Non-repudiation of participation. Every participant's approval is digitally signed and thus cannot be denied at any point in the future. The property guarantees the non-repudiation of participation, not the fact of the payment itself (Mbonu, 2020).

P3, Ordering integrity, conditional. The property holds for participants other than the orderer and does not hold for the orderer in the case of non-replicated ordering. Under the given topology, in which all orderers are subordinated to the treasury, the property does not hold for the treasury either.

P4, Retention independence. Since each full peer has its own copy of the block store, the destruction of storage of a single domain does not mean destruction of the trail. This makes the trail redundant in terms of storage (Fadayomi, 2019).

P5, Selective disclosure, incomplete. Both channel and private-data-collection mechanisms are able to exclude a record from some participants. That is required by confidentiality and toxic to auditability.

A payment deposited into a private collection is not included in the auditor's copy of the blockchain. Private transactions thus need their presence and hash logged on the public ledger (Onche, 2020; Mbonu, 2020).

5. Evaluation Harness Specification

None of the above has been done. This is done to fix the topology, chaincode, workload, metrics and faults scenarios in order to validate the design estimates of Section 6 with future measurements (Chiu, 2014).

5.1 Purpose and epistemic status

The harness described above is intended to answer one question: does a permissioned ledger offer tamper-resistance properties of Section 4 at the required throughput? The answer provided in this paper is a design estimate made based on the arithmetic of Section 6, rather than a measurement.

The specification is the tool used in the measurement study. Any deviation from the specification, in terms of topology, chaincode, workload or metrics, needs to be reported along with the findings. Continuous auditing literature provides theoretical background for an automation of audit capability (Rezaee, 2002; Chiu, 2014).

5.2 Network topology and chaincode

There are five organizations running two peers each, contributing one certificate authority. The treasury hosts the three-orderer Raft ordering service, there are two spending agencies, the external auditor has read-only chaincode, and the commercial bank contributes the payment

confirmation events. The total number of peers in the network is 10 and they belong to five administrative domains.

Ordering is the critical point here. All three orderers belong to one administrative domain, thus, the actual ordering trust domain is one domain and not 10 nodes or two domains. The independent-orderer scenario of Section 6.5 verifies this hypothesis (Kobelsky, 2014).

The specified hardware characteristics are 8 vCPUs and 32 GB of RAM for each peer. The inter-organization round-trip latency is 2 ms. This is a design parameter; there was neither injected nor measured any latency (Chiu, 2014).

The disbursement chaincode registers a payment transaction with its appropriation, obligation, invoice, and approval chains. Prior to committing, it verifies the balance with appropriation, the obligation state, the authorization of the approver, and checks the uniqueness of the invoice.

Each read and cross-reference check adds to the work done at endorsement, which is why the chaincode complexity factor γ in Section 6.1 is treated as a separate assumption. The specification fixes the business rules, but no compiled chaincode artifact has been run for this paper.

The payment checks are analogous to the controls implemented by accounts-payable systems (Einkamerer, 2017; Ali, 2016).

5.3 Workload generator

Volume. The volume on an annual basis is an assumption illustrative value of 186 million transactions that translates into 15.5 million transactions per month. This volume corresponds to 26 transactions per second assuming 250 days of 8 hours of work per business day.

Peak. The peak values of stress are 640 transactions per second for the last three days of a fiscal quarter, and 900 transactions per second for the last two business days of the fiscal year. Those are assumptions not referenced to any particular paper, and an operator is advised to use its own figures (Aifuwa, 2020).

The workload is synthetic stream generated according to the above assumptions. Payment mix, the payees' distribution, and rejection ratios will be determined in a measurement phase according to business rules from Section 5.2.

5.4 Metrics

M1, Peak Sustained Throughput At Defined Latency. The maximum rate of transactions per second when 99th-percentile commit latency remains under 2,000 milliseconds for ordinary payments and 5,000 milliseconds for milestones.

M2, Storage Growth Per Million Transactions. This measure is to be calculated independently for both state database and block store.

M3, Sensitivity of endorsement policy to throughput and latency. Throughput and latency for endorsement policies of 1-of-1, 2-of-4 and 3-of-5 among the five organizations.

M4, Cost of verification. Cost of verifying inclusion and integrity of a payment in the blockchain by depth: in the last block, last 1,000 blocks, or entire blockchain.

M4 is the metric of interest to auditing, because the verification that costs a lot to verify would be sampled (Power, 2013; Teeter, 2010).

5.5 Specified fault scenarios

For fault analysis, we have single peer failure in each organization, orderer failure, sixty second partition of ORG3, and orderer equivocation in a separate setup with four orderers. The latter two are only mentioned for future work. None of those has been implemented yet.

The partitioning scenario is most relevant to the custody case, because it checks whether the replica maintained by a partitioned node stays consistent with the rest of the network upon partition resolution. Offline evaluation of security critical systems does the same job (Ladapo, 2018). Orderer equivocation is testing the ordering assumption from 3.2 and property P3 from 4.4.

6. Synthesized Design Estimates

Each number here is a calculation based on the assumptions in Section 6.6; no data points have been measured (Batini, 2009).

6.1 Method of synthesis

Step 1. Take the throughput T_{kv} of the permissioned platform running simple key-value chaincode on comparable hardware. This is the upper bound on achievable rate. Its central value is 3,000 transactions per second, the midpoint of an assumed range of 2,400 to 3,600 transactions per second.

Step 2. Apply a chaincode complexity factor $\gamma \in (0,1]$ for the extra reads, cross-reference checks and business rules in the disbursement contract. The central value of γ is 0.55, within an assumed range of 0.45 to 0.70. No listed reference supplies this range.

Step 3. Apply an endorsement breadth factor β and a block parameter factor δ. Their central values are 0.51 for 3-of-5 endorsement and 1.00 for 2,000-transaction blocks, as given in Table 4.

The estimate is $T = T_{kv} \cdot \gamma \cdot \beta \cdot \delta$. We report ranges rather than point estimates, and every number in this section is a calculation from assumed inputs, not a measurement (Batini, 2009; Kogan, 2014).

6.2 Expected throughput

Table 1 reports the design estimates, which compare configurations before any measurement is taken (Kogan, 2014). With T_{kv} = 3,000 transactions per second and γ = 0.55, the 1-of-1 configuration reaches 1,650 transactions per second, the 2-of-4 configuration 1,188 and the 3-of-5 configuration 842 with 2,000-transaction blocks.

Table 1. Design estimates of peak throughput by configuration, assuming 3,000 tx/s central assumption for simple chaincode and 0.55 for complexity factor

Configuration	γ	β	δ	**Design estimate of peak (tx/s)**	**Meets 900 tx/s fiscal year-end peak?**
1-of-1 endorsement, 2,000-tx blocks	0.55	1.00	1.00	1,650	Yes
2-of-4 endorsement, 2,000-tx blocks	0.55	0.72	1.00	1,188	Yes
3-of-5 endorsement, 2,000-tx blocks	0.55	0.51	1.00	842	No
3-of-5 endorsement, 500-tx blocks	0.55	0.51	0.78	656	No
3-of-5 endorsement, 5,000-tx blocks	0.55	0.51	1.08	909	Yes, by 9 tx/s

Three observations can be made, and Section 6.5 examines to what extent they hinge on the complexity factor.

First, endorsement breadth is the dominant cost in the model. Moving from 1-of-1 to 3-of-5 multiplies the estimate by β = 0.51, which roughly halves it. Consensus is held fixed, so its effect is not compared.

Second, block parameter tuning recovers only part of the loss. Raising the block size from 2,000 to 5,000 transactions raises δ from 1.00 to 1.08, about 8 per cent, while reducing it to 500 transactions lowers δ to 0.78.

Third, the per-payment design works around the average throughput of about 26 tx/s but does not work well at the peak throughput. With 3-of-5 endorsement, the range of estimates goes from 656 tx/s to 909 tx/s versus 900 tx/s peak, which leaves little room for margin.

6.3 Expected latency

Table 2 gives design estimates of latency at 60 percent of saturation (99th percentile), based on the assumed phase budgets (Batini, 2009). The two numbers, 770 ms for 1-of-1 and 1,105 ms for 3-of-5, fit into the 2,000 ms goal of metric M1.

Table 2. Design estimates of latency phase budget at 60 per cent of saturation (milliseconds, 99th percentile)

Phase	**1-of-1 endorsement**	**3-of-5 endorsement**
Proposal and chaincode execution	180	180
Endorsement collection (parallel)	40	95
Ordering and block formation	310	310
Validation and commit	240	520
End-to-end	**770**	**1,105**

Ordering and block formation is the largest single phase under 1-of-1 endorsement, and its value depends on the block-cutting parameters in Section 9. Validation and commit grows disproportionately with endorsement breadth. Each of the ten peers verifies the endorsement signatures of every committed transaction, so a 3-of-5 policy generates 30 to 50 signature verifications per transaction, which is the mechanism behind the β factor in Table 1.

6.4 Storage growth

The table below shows design estimates of storage growth per million transactions in decimal units. Here, the block store refers to the total 1.00 KB as shown in section 6.7 while the state database is 0.90 KB and the index is 0.35 KB totaling 2.25 KB per transaction.

Table 3. Design estimates of storage growth per million disbursement transactions (decimal units; annual figures at 186 million payments per year)

Component	**Per transaction**	**Per million transactions**	**Per year at 186 million payments**
Block store: transaction payload (Section 6.7 subtotal)	0.94 KB	0.94 GB	174.8 GB
Block store: overhead (assumed allowance)	0.06 KB	0.06 GB	11.2 GB
Block store subtotal	1.00 KB	1.00 GB	186.0 GB
State database (current balances and	0.90 KB	0.90 GB	167.4 GB

references)			
Index	0.35 KB	0.35 GB	65.1 GB
Total	2.25 KB	2.25 GB	418.5 GB

With 186 million payments per year, one complete peer generates 186.0 GB of block store, 167.4 GB of state and 65.1 GB of index resulting in 418.5 GB. Ten complete peers generate 4.2 TB annually and 25.1 TB within six years. Validating peers must store the entire block store (Uzondu, 2020).

State is the current state, not the audit trail, and storing each payment in the state makes state storage increase linearly with volume (Curtis, 2012).

6.5 Sensitivity analysis

Chaincode complexity. Across the assumed range of γ from 0.45 to 0.70, the 3-of-5 estimate with 2,000-transaction blocks moves from about 690 to about 1,070 transactions per second. It reaches 900 only when γ exceeds about 0.59, so the per-payment design is marginal at peak for most of the range.

Inter-agency latency. The synthesis does not provide a quantification of its impact on the throughput. A 3-of-5 margin in 5,000-transaction blocks provides 9 transactions per second, which is approximately 1 per cent of the estimate. Thus, a decrease in such magnitude would remove the margin.

Domain of **independent** orderers. If orderers are put in an independent administrative domain, then their ordering trust base becomes an independent party rather than the treasury. The throughput effect is considered to be marginal and not computed in the model (Section 3.2).

Byzantine ordering. Four Byzantine fault-tolerant orderers are used to reduce the ordering throughput compared to Raft. No value for the reduction is assigned to this in the synthesis because the point of Byzantine ordering is its trust profile (Eyetsemitan, 2020).

6.6 Limits of the synthesis and conversion factors

The synthesis does not establish absolute capability. The factors T_{kv}, γ, β and δ are assumptions, and combining four assumed factors widens the uncertainty considerably. The ranges reported in Table 4 are design brackets, not confidence intervals.

A reader who needs an absolute number would need to conduct a measurement study of the specified harness. At present, only Tables 1 to 3 tell which configurations are worth measuring (Batini, 2009).

The sensitivity analysis in Section 6.5 shows which conclusions are still valid in the stated ranges. These are the only conclusions to be taken into the measurement study plan.

Table 4 gives the reason behind each conversion factor. None of them is taken from any benchmark in the reference list. As such, they are all explicit assumptions with an interval and a midpoint.

The complexity factor γ is the least constrained of the inputs, and the feasibility conclusion of Section 6.2 depends on it most, as Section 6.5 shows. A measurement study should therefore estimate γ first (Batini, 2009). The conversion chain is therefore only as firm as its least constrained factor, which Table 4 identifies.

Table 4. Reason behind each conversion factor (explicit assumptions; no factor is based on any listed benchmark)

Factor	Value range	Basis
T_{kv}	2,400 to 3,600 tx/s	Assumption. Central value 3,000 tx/s, the range midpoint. No listed reference reports a Fabric benchmark.
γ	0.45 to 0.70	Assumption. Central value 0.55. This is the least constrained input.
β (2-of-4)	0.68 to 0.76	Assumption. Central value 0.72. Each added endorsement adds verification cost at every peer.
β (3-of-5)	0.47 to 0.55	Assumption. Central value 0.51, extrapolated from the 2-of-4 range.
δ (500 tx blocks)	0.74 to 0.82	Assumption. Central value 0.78.
δ (5,000 tx blocks)	1.04 to 1.12	Assumption. Central value 1.08.
Ordering (Raft, 3 orderers)	Not throughput-limiting below saturation	Assumption. Not traced to a listed reference.

6.7 Storage and verification detail

The estimate of the block-store is as follows. Assuming that there are 420 bytes needed for the transaction envelope and signatures, with a transaction having 3-of-5 endorsements; 340 bytes for the chaincode write set for the payment fields; and 180 bytes for the hashed read set containing four read keys, we have a payload of 940 bytes. Also, assuming there is 60 bytes of

overhead due to headers, metadata, and validation flags makes it equal to 1,000 bytes. The size of the envelope is an assumption, not a measurement (Khan, 2010).

In Table 3, the 0.94 KB payload is the 940 bytes subtotal stated earlier, while the 60-byte overhead is an assumed overhead, not an actual header cost computed. Thus, the storage estimate is uncertain and a design estimate, not a measurement.

Operations are counted instead of being timed, since no measurements were made regarding them. A single payment involves the use of a Merkle path whose length is the base-two logarithm of the batch size. As such, about 19 hashes are required for a day's worth of about 510,000 payments. Block integrity requires one hash and one header parse, with 1,000 hash verifications and 1,000 header verifications required for the last 1,000 blocks.

Publication of checkpoint information by some participants will be the practical solution to full-chain cost, and this configuration lacks it (Power, 2013). The operations' numbers are design numbers, and the time when it will generate is yet to be recorded within the bounds of Section 5.

7. Cost, Governance, and Non-Performance Considerations

The following costs and governance situations limit the practical value of the ledger just as the through-put (Arumosoye, 2019).

7.1 Governance and incentives

A permissioned ledger is a consortium and requires a constitution defining membership, changes to policy, dispute resolution, and who covers failure on behalf of a participant (Arumosoye, 2019; Kranacher, 2011).

An auditor that has a replica and participates in governance is no longer completely independent from the network being audited (Eyetsemitan, 2020). In other words, an auditor must have a clearly defined position such as read-only observer.

When there is no clarity in governance, there is also no clarity in the allocation of responsibilities and failure costs. Governance agreement should define those prior to building the network (Dosunmu, 2019).

Participants benefit from a trusted record of their own transactions but incur the costs of running a peer. The network’s record is a public good, which consortia have an incentive to under-supply unless mandatory participation is required (Ilodigwe, 2019a). That is a classic free-rider problem that needs to be dealt with.

The design that will deal with that is a statutory allocation of the responsibility for operation of the ledger to independent entities. This is a policy decision rather than a technical one, and this paper does not assess its legal feasibility (Mbonu, 2019). In the absence of such allocation, the replication needed for the custody argument is based on good will.

7.2 Alternatives that should be compared

Append-only storage with external notarization. A traditional database periodically publishing the Merkle root to an independent external time stamping authority provides tamper proof against A4 and A5 at lower cost but the record still stays in one organization's custody (Okwesa, 2019).

Write-once storage with replication to an independent records authority under a records management agreement. Replication of the audit trail to an independent records authority ensures distributed custody without the complexity of the ledger but relies on enforcement of the agreement (Mbonu, 2019).

Both alternatives are not assessed quantitatively in this paper. A measurement study should include both of them as benchmarks for the ledger, since the custody argument in Section 4 makes sense only with respect to the least costly design that provides it (Mbonu, 2020).

8. Reference Architecture

The reference architecture splits the payment record, kept in conventional systems, from a cryptographic anchor recorded on the ledger. This is a design solution and has not been implemented (Oshoba, 2020).

8.1 The separation principle

According to Section 6, the per-payment ledger is marginal at the end of the fiscal year and increases with each payment made. According to Section 4, tamper resistance necessitates distributed custody of evidence, not copies of payment content. Thus, only commitments to payment detail get stored on the ledger, while the details themselves are kept in conventional systems (Mbonu, 2019; Alles, 2010).

The above separation of details and cryptographic anchors does not affect the custody argument, provided that all committed roots are replicated in independent domains. This way, all participants will have the same set of roots, while the payment detail will remain accessible to the auditor through the system of record (Khan, 2010).

8.2 Components

The payment system of record. Conventional transactional systems retain payments, balances and status and act as the system of record for audit details.

Batch committer. The committer, at intervals, performs computation of a Merkle tree over the payment records during a certain period and sends the ledger one transaction with its root, the number of payments and the period identifier. Batching daily gives 365 ledger transactions per year against 186 million payments, meaning a decrease by about 510,000 times. Batching hourly results in a decrease of about 21,000 (Khan, 2010).

Anchoring Ledger. The ledger records commitments and not payments. With an assumption that the commitment size is 1 KB, then there is an addition of 0.4 MB in case of daily batching and 8.8 MB in case of hourly batching compared to the 418.5 GB yearly per-payment storage in Table 3.

Disclosure and Verification Service. The verifier has the payment record and its Merkle path and performs checks by validating the path against the root in the ledger. This takes about 19 hash calculations in case of daily batching (Section 6.7).

Exception Channel. High-risk, high-value, adverse-matching, new payee and override payments are committed separately and in batch root. There should be an upper bound of the number of high-risk transactions before sizing the channel (Okwesa, 2019).

8.3 Properties of the architecture

All participants have the roots and, thus, all participants can recalculate the roots and check whether the committed record has been modified (Okwesa, 2019; Mbonu, 2019).

The design detects the modification of a committed record. However, the authenticity of the payment committed cannot be guaranteed since this is dependent on the control of the system of record. The payment archival responsibility lies with the system of record and its records management process (Singleton, 2010).

By not providing a way to query payments from the ledger, we have made a significant sacrifice. An auditor who needs to know details about some payment must look at the system of record and cross-check it with the committed root (Teeter, 2010).

8.4 The duplicate payment problem and a partial resolution

An approximate solution involves placing the ledger under a restricted shared state that contains the duplication keys: invoice ids, obligation ids, and payee-amount-date triples. Each of the keys is put as a claim with a short lock duration (Okonkwo, 2019; Coderre, 2009). We keep the keys narrow in order to make the shared state small.

Since each claim not cleared would block a payment, the expiry and reconciliation process is necessary (Okonkwo, 2019; Khan, 2009). Each claim is also an additional write operation that increases the endorsement load discussed in Section 6, and the volume of this operation should be calculated prior to adopting the design. The lock duration is one of the design parameters that are not estimated in this paper.

8.5 Audit procedures permitted and foreclosed

Full population **verification.** Inclusion verification is performed by a simple root lookup, thus allowing the auditor to verify all payments within a period, and not sample them (Power, 2013).

Proof of non-suppression. An auditor could prove that the number of payments committed in a period equals to the number reported by the system of record.

Proof of temporality. Since the commitments occur periodically and the orderings are set, the auditor is able to determine the point of existence of the record (Alles, 2008).

The design precludes two processes. It prevents going through the payment details from the ledger and checking the commitment against the reality of the payment (Okonkwo, 2019; Alles, 2008).

9. Full Harness Configuration

The above configuration presumes the usage of a three-orderers' Raft ordering service within one administrative domain, gossip propagation and LevelDB as state database. These options are presumed to be used in a Hyperledger Fabric release and they were not verified against any particular version.

The block parameters are specified design settings, not defaults taken from a published source. The default configuration sets 2,000 transactions per block, a 2 s absolute timeout and 10 MB preferred maximum bytes; the small-block configuration sets 500 transactions, 1 s and 2 MB; the large-block configuration sets 5,000 transactions, 2 s and 20 MB; and the latency-optimized configuration sets 200 transactions, 500 ms and 1 MB. The latency-optimized configuration is a specified alternative for a measurement study, and each configuration is a candidate input to the block parameter factor δ in Section 6.1 (Rezaee, 2002; Chiu, 2014).

10. Cost Model

The following estimates are the design assumptions and not the real costs but they indicate where the efforts are expected (Adeyemi, 2019).

10.1 Per-participant recurring cost

The costs incurred by each participant annually in a case of a five-participant and ten-peers network are as follows. Infrastructure costs (compute, storage and networking) are considered low for a small participant and moderate for a large one. Operations of the certificate authority are low for both. The costs of membership management are 0.2 FTE for a small participant and 0.35 FTE for a large one, incident response and patches are 0.15 and 0.3 and governance participation costs are 0.1 and 0.2. The storage growth at the horizon of retention is moderate for both. In total it comes to approximately 0.45 FTE for a small participant and 0.85 for a large one.

Here, the recurring costs come down to personnel work. That is why smaller enterprises will be unable to engage fully as peers, and such engagement should typically be mandated at network level (Stamatović, 2020). The cost per participant depends on the assumed premises and inherits their uncertainty.

11. Conclusion

Permissioned distributed ledgers offer an explicit feature for government disbursements audit trails: distributed custody of evidence in the sense that no one participant may tamper with, suppress or selectively disclose a record without being discovered by some other participant. The feature relies on replication across administrative domains, rather than on the chain.

The feature does not cover immutability usually mentioned in this context. It gives very little protection against a treasury operating the ordering service and it tells us nothing about the truthfulness of a record.

In design estimates, endorsement width prevails over throughput, and a simple per-payment design falls short of the peak seen at fiscal year end. The separation design of Section 8 allows keeping payment data in legacy systems and posting Merkle roots at intervals on the ledger.

This separation design preserves the feature needed, limits ledger storage and allows for full population verifications. The ledger guarantees that a record has remained unchanged from the time when its root has been committed. It tells us nothing about the authenticity of the record. Now it is time to measure the specified harness.

References

The paper contains a total of 200 sources of information: 100 references from the customer's reference library prepared for this project and 100 references obtained by the author himself through literature search. Each of the cited works is dated 2020 and before, which is the threshold indicated in the title of the current paper.

1. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E., 2020. A Conceptual Framework for Agile Supply Chain Digital Transformation with Embedded IT Risk and ISO Compliance Controls. Iconic Research and Engineering Journals, 3(11), pp.566–593. DOI: 10.64388/IREV3I11-1714916.
2. Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(5), 371–389. https://doi.org/10.32628/IJSRCSEIT
3. Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 371-389.
4. Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 371-389.

5. Orise, C., & Niniola, S. (2020). Data-informed digital learning platforms: A conceptual framework for evidence-based educational technology in healthcare and STEM environments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1078-1089. https://doi.org/10.54660/.IJMRGE.2020.1.5.1078-1089
6. Orise, C., & Niniola, S. (2020). Data-informed digital learning platforms: A conceptual framework for evidence-based educational technology in healthcare and STEM environments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1078-1089. https://doi.org/10.54660/.IJMRGE.2020.1.5.1078-1089
7. Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. Journal of Frontiers in Multidisciplinary Research, 1(1), 193-201.
8. Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. Journal of Frontiers in Multidisciplinary Research, 1(1), 193-201.
9. Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability limitations, advances and future research opportunities. Iconic Research and Engineering Journals, 2(12), 602–617. https://doi.org/10.64388/IREV2I12-1713779
10. Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. Iconic Research and Engineering Journals, 2(12), 602-617. https://doi.org/10.64388/IREV2I12-1713779
11. Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. Iconic Research and Engineering Journals, 2(12), 602-617. https://doi.org/10.64388/IREV2I12-1713779
12. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911
13. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911
14. Mbonu, I.S., Aliliele, C., Iwuanyanwu, U. & Oluoha, O.M., 2018. A Conceptual Framework for Legal and Ethical Risk Modeling in Enterprise Data Protection Governance Systems. Iconic Research and Engineering Journals, 2(2), pp.207–226. DOI: 10.64388/IREV2I2-1714911

15. Adaramola, T. S., Fadero, S., & Gideon, E. N. (2020). Machine learning and data-driven approaches in industrial automation and process control. International Journal of Engineering and Modern Technology, 6(3), 103–128.
16. Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., Ike, P. N., Nnabueze, S. B., & Olatunde-Thorpe, J. (2020). Predictive analytics models enhancing accuracy of demand forecasting in supply chains and minimising inefficiencies in inventory management. International Journal of Multidisciplinary Research and Growth Evaluation, 1(3), 171–181. https://doi.org/10.54660/.IJMRGE.2020.1.3.171-181
17. Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., Ike, P. N., Nnabueze, S. B., & Olatunde-Thorpe, J. (2020). Predictive analytics models enhancing accuracy of demand forecasting in supply chains and minimising inefficiencies in inventory management. International Journal of Multidisciplinary Research and Growth Evaluation, 1(3), 171-181. https://doi.org/10.54660/.IJMRGE.2020.1.3.171-181
18. Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., Ike, P. N., Nnabueze, S. B., & Olatunde-Thorpe, J. (2020). Predictive analytics models enhancing accuracy of demand forecasting in supply chains and minimising inefficiencies in inventory management. International Journal of Multidisciplinary Research and Growth Evaluation, 1(3), 171-181. https://doi.org/10.54660/.IJMRGE.2020.1.3.171-181
19. Arumosoye, O. M., & Obriki, O. D. (2020). A governance-based model for assessing safety performance of contractors in multi-contract industrial projects. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 728-740. https://doi.org/10.54660/.IJMRGE.2020.1.5.728-740
20. Arumosoye, O. M., & Obriki, O. D. (2020). A governance-oriented conceptual model for contractor safety performance in multi-contract industrial projects. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 728-740. https://doi.org/10.54660/.IJMRGE.2020.1.5.728-740
21. Arumosoye, O.M. & Obriki, O.D., 2020. A Governance-Oriented Conceptual Model for Contractor Safety Performance in Multi-Contract Industrial Projects. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp.728-740. DOI: 10.54660/.IJMRGE.2020.1.5.728-740
22. Asibor, E., & Isong, D. E. (2020). Flare-gas recovery technologies for advancing energy security, environmental performance, and resource efficiency. Iconic Research and Engineering Journals, 4(1), 369-410. https://doi.org/10.64388/IREV4I1-1723154
23. Asibor, E. & Isong, D.E., 2020. Flare-Gas Recovery Technologies for Advancing Energy Security, Environmental Performance, and Resource Efficiency. IRE Journals, 4(1), pp.369-410. DOI: 10.64388/IREV4I1-1723154.
24. Atakpa, M. I., & Abolaji, T. (2020). Data-driven health equity: A proposed framework for analytics-based health needs assessment in underserved communities. Iconic Research and Engineering Journals, 4(5), 410-432. https://doi.org/10.64388/IREV4I5-1718410

25. Atakpa, M.I. & Abolaji, T., 2020. Data-Driven Health Equity: A Proposed Framework for Analytics-Based Health Needs Assessment in Underserved Communities. IRE Journals, Iconic Research and Engineering Journals, 4(5), pp.410–432. DOI: 10.64388/IREV4I5-1718410.
26. Boakye, K., Ofori, S. D., Ogbona, C. S., Yeboah, T. J., & Bobga, M. A. (2020). Integrating ICT and mathematical thinking: Exploring the effectiveness of digital tools in secondary mathematics instruction. Iconic Research and Engineering Journals, 4(4), 372-398. https://doi.org/10.64388/IREV4I4-1714179
27. Boakye, K., Ofori, S. D., Ogbona, C. S., Yeboah, T. J., & Bobga, M. A. (2020). Integrating ICT and mathematical thinking: Exploring the effectiveness of digital tools in secondary mathematics instruction. Iconic Research and Engineering Journals, 4(4), 372-398. https://doi.org/10.64388/IREV4I4-1714179
28. Eyetsemitan, R. A., Ambali, K. B., Oyeleye, A. O., & Fadayomi, O. (2020). Multi-stakeholder governance alignment in joint venture operations: A conceptual framework for coordinating business processes in highly regulated environments. Iconic Research and Engineering Journals, 4(4), 418-441. https://doi.org/10.64388/IREV4I4-1716955
29. Eyetsemitan, R. A., Ambali, K. B., Oyeleye, A. O., & Fadayomi, O. (2020). Multi-stakeholder governance alignment in joint venture operations: A conceptual framework for coordinating business processes in highly regulated environments. Iconic Research and Engineering Journals, 4(4), 418-441. https://doi.org/10.64388/IREV4I4-1716955
30. Eyetsemitan, R. A., Ambali, K. B., Oyeleye, A. O., & Fadayomi, O. (2020). Multi-stakeholder governance alignment in joint venture operations: A conceptual framework for coordinating business processes in highly regulated environments. IRE Journals, 4(4), 418-441. DOI: 10.64388/IREV4I4-1716955
31. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2020). A conceptual supply chain talent development model for capability building across distributed operations. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 439-456. https://doi.org/10.54660/.ijmrge.2020.1.5.439-456
32. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2020). A conceptual supply chain talent development model for capability building across distributed operations. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 439-456. https://doi.org/10.54660/.ijmrge.2020.1.5.439-456
33. Izuchukwu, O. T., Feboh, D., & Ajirotutu, A. (2020). Comprehensive review of automated building code compliance and digital permitting systems in architecture. International Journal of Engineering and Modern Technology, 6(3), 103-125. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg103.125
34. Izuchukwu, O. T., Feboh, D., Ijagbemi, A. O., Oyefuga, M., & Nwakamma, S. (2020). Digital transformation of facility and property management: Integrating business intelligence tools for cost reduction in emerging markets. International Journal of Multidisciplinary

Research and Growth Evaluation, 1(5), 1107-1117. https://doi.org/10.54660/.IJMRGE.2020.1.5.1107-1117

35. Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020b). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 811-828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828
36. Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020b). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 811-828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828
37. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E., 2020. Advances in Infrastructure as Code Governance for Secure Terraform Based Enterprise Cloud Deployments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp.811–828. DOI: 10.54660/IJMRGE.2020.1.5.811-828.
38. Okojie, J. S., Filani, O. M., Ihwughwavwe, S. I., & Sakyi, J. K. (2020). Sustainable procurement practices: ESG-integrated supply chain models for corporate responsibility and environmental performance. IRE Journals, 4(2).
39. Okojie, J. S., Filani, O. M., Ihwughwavve, S. I., & Sakyi, J. K. (2020). Sustainable procurement practices: ESG-integrated supply chain models for corporate responsibility and environmental performance. IRE Journals, 4(2).
40. Okojie, J. S., Filani, O. M., Ihwughwavwe, S. I., & Sakyi, J. K. (2020). Sustainable procurement practices: ESG-integrated supply chain models for corporate responsibility and environmental performance. IRE Journals, 4(2).
41. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1032-1044. https://doi.org/10.54660/.IJMRGE.2020.1.5.1032-1044
42. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1032-1044. https://doi.org/10.54660/.IJMRGE.2020.1.5.1032-1044
43. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1032-1044. https://doi.org/10.54660/.IJMRGE.2020.1.5.1032-1044
44. Sanni, J. O., Ajiga, D., & Atima, M. E. (2020b). Data driven brand positioning frameworks resolving differentiation challenges in regulated professional markets. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 649-660. https://doi.org/10.54660/IJMRGE.2020.1.5.649-660

45. Sanni, J. O., Ajiga, D., & Atima, M. E. (2020b). Data driven brand positioning frameworks resolving differentiation challenges in regulated professional markets. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 649-660. https://doi.org/10.54660/IJMRGE.2020.1.5.649-660
46. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2020). Force majeure and contractual resilience in global energy supply chains: A systematic review. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1247-1264. https://doi.org/10.54660/.IJMRGE.2020.1.5.1247-1264
47. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2020). Force majeure and contractual resilience in global energy supply chains: A systematic review. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1247-1264. https://doi.org/10.54660/.IJMRGE.2020.1.5.1247-1264
48. Uzondu, C. S., Ibeh, A. V., Alugwe, S., & Awulu, I. (2020). Corporate credit portfolio growth in emerging markets: A review of advances in credit decisioning and governance. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1279-1294. https://doi.org/10.54660/.IJMRGE.2020.1.5.1279-1294
49. Uzondu, C. S., Ibeh, A. V., Alugwe, S., & Awulu, I. (2020). Corporate credit portfolio growth in emerging markets: A review of advances in credit decisioning and governance. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1279-1294. https://doi.org/10.54660/.IJMRGE.2020.1.5.1279-1294
50. Agbabiaka, J., Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2019). Supply chain risk management model for EPC and gas processing projects. Iconic Research and Engineering Journals, 3(2), 968-980. https://doi.org/10.64388/IREV3I2-1713124
51. Agbabiaka, J., Okonkwo, C.S., Ogunwole, O., Mayo, W. & Okeke, O.T., 2019. Supply Chain Risk Management Model for EPC and Gas Processing Projects. IRE Journals, 3(2), pp.968–980. DOI: 10.64388/IREV3I2-1713124.
52. Agyei, R. K., Izuchukwu, O. T., Feboh, D., & Idowu, A. (2019). Determinants of web-based payment portal adoption in Sub-Saharan Africa: A review and synthesis. International Journal of Computer Science and Mathematical Theory, 5(2), 56-79. https://doi.org/10.56201/ijcsmt.vol.5.no2.2019.pg56.79
53. Agyei, R. K., Izuchukwu, O. T., Feboh, D., & Idowu, A. (2019). Determinants of web-based payment portal adoption in Sub-Saharan Africa: A review and synthesis. International Journal of Computer Science and Mathematical Theory, 5(2), 56-79. https://doi.org/10.56201/ijcsmt.vol.5.no2.2019.pg56.79
54. Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. Iconic Research and Engineering Journals, 3(2), 981-999. https://doi.org/10.64388/IREV3I2-1714417
55. Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. Iconic Research and Engineering Journals, 3(2), 981-999. https://doi.org/10.64388/IREV3I2-1714417

56. Arumosoye, O.M. & Obriki, O.D., 2019. Systematic Review of Near-Miss and Hazard Observation Data Utilization in Industrial Safety Management. IRE Journals, 3(2), pp.981–999. DOI: 10.64388/IREV3I2-1714417
57. Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225
58. Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225
59. Ijagbemi, A. O., Izuchukwu, O. T., Feboh, D., Nwakamma, S., & Oyefuga, M. (2019). Data-driven performance monitoring in maritime logistics: A framework for improving operational efficiency in developing-economy ports. Iconic Research and Engineering Journals, 3(6), 630–649. https://doi.org/10.64388/IREV3I6-1722787
60. Ilodigwe, L., & Adesemoye, A. C. (2019a). A critical review of health insurance financing mechanisms and provider payment reform strategies for balancing coverage expansion and financial protection in emerging markets. International Journal of Health and Pharmaceutical Research, 5(2), 31-55. https://doi.org/10.56201/ijhpr.vol.5.no2.2019.pg31.55
61. Ilodigwe, L., & Adesemoye, A. C. (2019a). A critical review of health insurance financing mechanisms and provider payment reform strategies for balancing coverage expansion and financial protection in emerging markets. International Journal of Health and Pharmaceutical Research, 5(2), 31-55. https://doi.org/10.56201/ijhpr.vol.5.no2.2019.pg31.55
62. Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals, 2(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912
63. Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals, 2(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912
64. Mbonu, I.S., Aliliele, C., Uzoka, E. & Oluoha, O.M., 2019. A Review of Comparative Data Protection Regulations and Secure Cloud Implementation Strategies Across Jurisdictions. Iconic Research and Engineering Journals, 2(9), pp.482–501. DOI: 10.64388/IREV2I9-1714912.
65. Obogo, S.F., Ozobu, C.O. & Uduokhai, D.O., 2019. Development of a Construction Safety Risk Governance Model for Multi Contractor High Rise Projects. Iconic Research and Engineering Journals, 2(9), pp.502-522. DOI: 10.64388/IREV2I9-1715495
66. Odejobi, O. D., Hammed, N. I., & Ahmed, K. S. (2019). Approximation complexity model for cloud-based database optimization problems. IRE Journals, 2(9), 1-10.
67. Odejobi, O. D., Hammed, N. I., & Ahmed, K. S. (2019). Approximation complexity model for cloud-based database optimization problems. IRE Journals, 2(9), 1-10.

68. Ojeakhena, F., Okeke, E.C., Komi, M., Ogunnowo, E., Ogundapo, O. & Ibe, P.N., 2019. Architectural Models for Automated Diagnostic Logging, Fault Detection, and Data Persistence in Industrial Embedded Systems. International Journal of Humanities and Information Technology, Special Issue 3, pp.146–155. DOI: 10.21590/ijhit.spcl.03.06.
69. Okonkwo, C. S., Ogunwole, O., Okeke, O. T., & Mayo, W. (2019). Conceptual framework for cost reduction through contract negotiation and vendor governance. Iconic Research and Engineering Journals, 2(9), 468-482. https://doi.org/10.64388/IREV2I9-1713121
70. Okonkwo, C., Ogunwole, O., Okeke, O. T., & Mayo, W. (2019). Conceptual framework for cost reduction through contract negotiation and vendor governance. Iconic Research and Engineering Journals, 2(9), 468-482. doi: 10.64388/IREV2I9-1713121.
71. Okonkwo, C., Ogunwole, O., Okeke, O. T., & Mayo, W. (2019). Conceptual Framework for Cost Reduction Through Contract Negotiation and Vendor Governance. IRE Journals, 2(9), pp. 468-482. DOI: 10.64388/IREV2I9-1713121.
72. Okwesa, I. J., Ajiga, D., & Iwuanyanwu, U. (2019). Automation of log collection and incident triage for security operations: A review. Iconic Research and Engineering Journals, 3(5). doi: 10.64388/IREV3I5-1722629
73. Okwesa, I.J., Ajiga, D. & Iwuanyanwu, U., 2019. Automation of Log Collection and Incident Triage for Security Operations: A Review. Iconic Research and Engineering Journals, 3(5). DOI: 10.64388/IREV3I5-1722629.
74. Unamma, U. M.-L., Okwesa, I. J., & Iwuanyanwu, U. (2019a). Data-quality and single-source-of-truth frameworks for inter-agency reporting: A review. International Journal of Social Sciences and Management Research, 5(4), 108-131. https://doi.org/10.56201/ijssmr.vol.5no4.2019.pg108.131
75. Unamma, U. M.-L., Okwesa, I. J., & Iwuanyanwu, U. (2019b). A Typology of Digital Complaint-Resolution Systems for Public Accountability. Journal of Public Administration and Social Welfare Research, 4(1), 50-76. https://doi.org/10.56201/jpaswr.v4.no1.2019.pg50.76
76. Unamma, U.M-L., Okwesa, I.J. & Iwuanyanwu, U., 2019. A Typology of Digital Complaint-Resolution Systems for Public Accountability. Journal of Public Administration and Social Welfare Research, 4(1), pp.50-76. DOI: 10.56201/jpaswr.v4.no1.2019.pg50.76.
77. Unamma, U.M-L., Okwesa, I.J. & Iwuanyanwu, U., 2019. Data-Quality and Single-Source-Of-Truth Frameworks for Inter-Agency Reporting: A Review. International Journal of Social Sciences and Management Research, 5(4), pp.108–131. DOI: 10.56201/ijssmr.vol.5no4.2019.pg108.131.
78. Adeyelu, O. O. (2018). A Predictive Compliance Monitoring Framework for Detecting Systemic Safety Risks through Aviation Consumer Complaint Data. Iconic Research and Engineering Journals, 1(8), 250-276. https://doi.org/10.64388/IREV1I8-1718478
79. Adeyelu, O. O. (2018). A Predictive Compliance Monitoring Framework for Detecting Systemic Safety Risks through Aviation Consumer Complaint Data. Iconic Research and Engineering Journals, 1(8), 250-276. https://doi.org/10.64388/IREV1I8-1718478

80. Adeyelu, O.O., 2018. A Predictive Compliance Monitoring Framework for Detecting Systemic Safety Risks Through Aviation Consumer Complaint Data. Iconic Research and Engineering Journals, 1(8), pp.250-276. DOI: 10.64388/IREV1I8-1718478.
81. Agboada, P., Ezeako, R., Okoli, I. E., & Uzondu, C. S. (2018). Digital transformation in operations management: A review of advances in automation, analytics, and process redesign. International Journal of Engineering Technology Research & Management, 2(11), 109-134.
82. Agboada, P., Ezeako, R., Okoli, I. E., & Uzondu, C. S. (2018). Digital transformation in operations management: A review of advances in automation, analytics, and process redesign. International Journal of Engineering Technology Research & Management, 2(11), 109-134.
83. Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. Iconic Research and Engineering Journals, 1(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778
84. Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. Iconic Research and Engineering Journals, 1(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778
85. Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual Model for Insider Threat Classification and Risk Modeling in Complex Digital Systems. Iconic Research and Engineering Journals, 1(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778
86. Azeez, L. O., & Badmus, O. B. (2018). Data-driven framework for predicting subsurface contamination pathways in complex remediation projects. Iconic Research and Engineering Journals, 2(5), 312-335.
87. Azeez, L. O., & Badmus, O. B. (2018). Data-driven framework for predicting subsurface contamination pathways in complex remediation projects. Iconic Research and Engineering Journals, 2(5), 312-335.
88. Dagodzo, D. (2018). Hydrothermal Alteration Interpretation of LANDSAT and ASTER Data. Saarbrücken, Germany: Lambert Academic Publishing. ISBN: 978-3-330-02903-3
89. Ekemezie, U. C., Ohunyon, G., & Sydney, E. (2018). Evaluating IDSR implementation in Benue State, Nigeria: DHIS2 data quality and surveillance capacity. Iconic Research and Engineering Journals, 2(6).
90. Ekemezie, U. C., Ohunyon, G., & Sydney, E. (2018). Implementation of IDSR in Benue State of Nigeria: DHIS2 data quality and surveillance capacity. Iconic Research and Engineering Journals, 2(6).
91. Fadero, S., Oyesiji, S. O., Nwakamma, S., & Jooda, D. (2018). IT governance frameworks (COBIT/ITIL) and their role in compliance with regulations by insurance companies in Nigeria. IRE Journals, 2(5), 478–496.

92. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned through offline assessment of security-critical systems: A case study of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205
93. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned through offline assessment of security-critical systems: A case study of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205
94. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned through offline assessment of security-critical systems: A case study of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205
95. Lamidi, O. B. A., & Olamide, A. (2018). Spatially explicit risk modeling framework for tracking subsurface contaminant migration in data-limited remediation sites. Iconic Research and Engineering Journals, 2(6), 178-198.
96. Lamidi, O. B. A., & Olamide, A. (2018). Spatially explicit risk modeling framework for tracking subsurface contaminant migration in data-limited remediation sites. Iconic Research and Engineering Journals, 2(6), 178-198.
97. Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. Iconic Research and Engineering Journals, 1(7), 169-189. https://doi.org/10.64388/IREV1I7-1714414
98. Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. Iconic Research and Engineering Journals, 1(7), 169-189. https://doi.org/10.64388/IREV1I7-1714414
99. Obriki, O.D. & Arumosoye, O.M., 2018. Conceptual Modeling of Data-Driven Occupational Safety Risk Control in Large-Scale Energy Infrastructure Projects. IRE Journals, 1(7), pp.169–189. DOI: 10.64388/IREV1I7-1714414
100. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2018). Optimization of laboratory space planning techniques for enhancing accuracy, safety, and efficiency of diagnostics. Iconic Research and Engineering Journals, 2(1), 87-113. https://doi.org/10.64388/IREV1I7-1713587
101. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explanation of the prediction of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144.
102. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the contemporary audit: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.
103. Alles, M., & Gray, G. L. (2016). The incorporation of big data into audits: Identifying barriers and research agenda addressing these barriers. International Journal of Accounting Information Systems, 22, 44-59.

104. Kiesow, A., Schomaker, T., & Thomas, O. (2016). Continuous auditing in the digital era: The state of knowledge after 30 years of research. Proceedings of the European Conference on Information Systems.
105. Aalst, van der. Process Mining: Data Science in Action (2nd Ed.). Springer. 2016
106. Akoglu, L., Tong, H., & Koutra, D. Graph based anomaly detection and description: A survey. Data Mining and Knowledge Discovery. Vol. 29, Issue 3, pp. 626-688.
107. Alles, M.G. Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. Accounting Horizons. Vol. 29, Issue 2, pp. 439-449.
108. Vasarhelyi, M.A., Kogan, A., & Tuttle, B.M. Big data in accounting: An overview. Accounting Horizons. Vol. 29, Issue 2, pp. 381-396.
109. Wang, T. & Cuthbertson, R. Eight issues on audit data analytics we would like researched. Journal of Information Systems. Vol. 29, Issue 1, pp. 155-162.
110. Gray, G. L., & Debreceny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. International Journal of Accounting Information Systems, 15(4), 357-380.
111. Haney, C., & Phelps, D. (2014). Responding to CMS overpayment demands: Practical steps for an appeal. The Health Lawyer, 26(6), 21-28.
112. Kogan, A., Alles, M. G., Vasarhelyi, M. A., & Wu, J. (2014). Design and evaluation of a continuous data level auditing system. Auditing: A Journal of Practice & Theory, 33(4), 221-245.
113. Provost, F., & Fawcett, T. (2013). Data Science for Business. O'Reilly Media.
114. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188.
115. Christen, P. (2012). Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection. Springer.
116. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.
117. Binder, C. (2011). Medicare program integrity: Activities to protect Medicare from payment errors, fraud, and abuse. Congressional Research Service Report R41526.
118. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.
119. Debreceny, R. S., & Gray, G. L. (2010). Data mining journal entries for fraud detection: An exploratory study. International Journal of Accounting Information Systems, 11(3), 157–181.
120. Jans, M., Lybaert, N., & Vanhoof, K. (2010). Fraud risk reduction in the internal fraud: A data mining case study. International Journal of Accounting Information Systems, 11(1), 17-41.
121. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.

122. Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for data quality assessment and improvement. ACM Computing Surveys, 41(3), 1-52.
123. He, H., & Garcia, E. A. (2009). Learning from imbalanced data sets. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263-1284.
124. Sparrow, M. K. (2008). Fraud in the US healthcare system: The vulnerabilities of automated payment systems. Social Research, 75(4), 1151-1180.
125. Ashcroft, P. (2002). Use of digital analysis in the audit process. Today's CPA, 32(4), 26-30.
126. Zadrozny, B., & Elkan, C. (2002). Transformation of classification scores to produce accurate multiclass probability estimates. Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 694-699.
127. Nigrini, M. J. (2000). Digital Analysis using Benford's Law: Tests and Statistics for Auditors. Global Audit Publications.
128. Agrawal, R., & Srikant, R. (1994). Efficient algorithms for mining association rules. Proceedings of the 20th International Conference on Very Large Data Bases, 487-499.
129. Landis, J. R., & Koch, G. G. (1977). Measurement of observer agreement for categorical data. Biometrics, 33(1), 159-174.
130. Chen, Z. X., Hohmann, L., Banjara, B., & Zhao, Y. (2020). Suggestions to protect patients and health care practices from Medicare and Medicaid fraud. Journal of the American Pharmacists Association, 60(4), e1-e8.
131. Stamatović, M., & Maksimović, S. (2020). Risk management as an integral part of internal financial control system: Case of public sector in Serbia. Economy and Market Communication Review, 10(2).
132. Adeyemi, F. K., & Olarewaju, O. M. (2019). Internal control system and financial accountability: A study of the public sector in Nigeria South-Western. Acta Universitatis Danubius: Oeconomica, 15(1), 45-62.
133. Hamdan, K. H. (2019). Application of COSO internal control framework in disaster management assessment in Iraq. Muthanna Journal of Administrative and Economic Sciences, 9(2).
134. Ujkani, S., & Vokshi, N. B. (2019). An Overview about the evolution of internal control in the public sector: The case of Kosovo. University of Malta.
135. Donley, G. (2018). The broken Medicare appeals system: Regulatory failures and the possibilities of litigation. Health Matrix, 28, 107-146.
136. Gonzalez, G. C., & Hoffman, V. B. (2018). Auditee impacts of electronic vs face-to-face contact in continuous auditing. Journal of Forensic & Investigative Accounting, 10(1), 92-110.
137. Kogan, A., Alles, M. G., & Vasarhelyi, M. A. (2018). Analytical procedures in auditing: A review and research framework. Journal of Accounting Literature, 40, 83-101.
138. Lopez, J., & Rubio, J. E. (2018). Access control for cyber-physical systems interconnected to the cloud. Computer Networks, 134, 46-54.

139. Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1-10.
140. Einkamerer, T. F., & Maqbool, J. (2017). Accounts Payable: Improving the Efficiency of a System. Applied Management Review, 2(1), 45-58.
141. Kirk, K. M. (2017). Predictive Model Analysis of Medicare and Medicaid Inpatient Stays and Recovery Audit Contracting Program. Rutgers University.
142. Lundberg, S. M., & Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.
143. Mohammed, M. A. (2017). Framework to design, implement and perform an effective internal control system. Ankara Yıldırım Beyazıt University.
144. Ali, N. (2016). E-invoicing adaptation: Benefits, challenges and strategies to overcome challenges in the future. Helsinki Metropolia University of Applied Sciences.
145. Issa, H., Ting, S., & Vasarhelyi, M. A. (2016). Artificial intelligence in auditing research: Formalizing audit and augmenting workforces. Journal of Emerging Technologies in Accounting, 13(2), 1-20.
146. Lee, H. C. (2016). Will electronic tax invoicing enhance tax compliance? The experience of the Republic of Korea's electronic tax invoicing for value-added tax. World Bank Policy Research Working Paper 7592.
147. Hardy, C. A., & Laslett, G. (2015). Continuous auditing and monitoring in practice: Insights gained from Metcash's business assurance group. Journal of Information Systems, 29(2), 183-194.
148. King, K. M. (2015). Medicare Part D: Modifications needed to improve CMS recovery audit program operations and contractor oversight (GAO-15-633). U.S. Government Accountability Office.
149. Chiu, V. (2014). The evolution and intellectual structure of continuous auditing research. Journal of Accounting Literature, 33, 37-57.
150. Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. ACM Computing Surveys, 46(4), 1-37.
151. Jans, M., van der Werf, J. M., Lybaert, N., & Vanhoof, K. (2014). A business process mining application for internal transaction fraud mitigation. Expert Systems with Applications, 38(10), 13351-13359.
152. Kobelsky, K. (2014). A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-based processes. International Journal of Accounting Information Systems, 15(4), 300-311.
153. Babatunde, S. A. (2013). Stakeholders' perception on the effectiveness of internal control system on financial accountability in the Nigerian public sector. International Journal of Business and Management Invention, 2(1), 16-33.
154. Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal Control—Integrated Framework. COSO.

155. Jans, M., Alles, M. G., & Vasarhelyi, M. A. (2013). Process mining in auditing: Sources of value added and areas of application. International Journal of Accounting Information Systems, 14(1), 1-20.
156. Power, M. (2013). The audit society: Rituals of verification (2nd ed.). Oxford University Press.
157. Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2012). Fraud Examination (4th ed.). Cengage Learning.
158. Curtis, M. B., & Turley, S. (2012). The business risk audit: A longitudinal field study of an audit engagement. Accounting, Organizations and Society, 37(7), 439-460.
159. Dorminey, J., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2012). The evolution of fraud theory. Issues in Accounting Education, 27(2), 555-579.
160. Nigrini, M. J. (2012). Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection. Wiley.
161. Reginato, E., Nonnis, C., & Pavan, A. (2012). Modern public internal control systems and accountability in health care organisations. Economia Aziendale Online, 3(2), 149-160.
162. Zhang, C., Pawlicki, A., McReynolds, D., & Titera, W. (2012). A continuous auditing web services model for XML-based accounting systems. International Journal of Accounting Information Systems, 13(2), 55-79.
163. Kranacher, M.-J., Riley, R. A., & Wells, J. T. (2011). Forensic Accounting and Fraud Examination. Wiley.
164. Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19-50.
165. Perols, J. L., & Lougee, B. A. (2011). Earnings management and financial statement fraud: An empirical analysis. Advances in Accounting, 27(1), 39-53.
166. Trotman, K. T., & Wright, A. (2011). Triangulation of audit evidence for fraud risk assessments. Accounting, Organizations and Society, 37(1), 41-53.
167. Wells, J. T. (2011). Corporate Fraud Handbook: Prevention and Detection (3rd ed.). Wiley.
168. Zhou, W., & Kapoor, G. (2011). Evolutionary detection of financial statement fraud. Decision Support Systems, 50(3), 570-575.
169. Van der Aalst, W. M. P. (2011). Process Mining: Discovery, Conformance and Enhancement of Business Processes. Springer.
170. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2010). Audit Automation and its Principles and Problems as a Precursor to Continuous Auditing. Working Paper, Rutgers University.
171. Dilla, W. N., & Janvrin, D. J. (2010). Where do experts look?: Eye-tracking investigation into search processes in estimate audits. Journal of Information Systems, 24(2), 25-48.
172. Khan, R., Corney, M., Clark, A., & Mohay, G. (2010). Transaction Mining for Fraud Detection in ERP Systems. Information Systems Management, 27(2), 141–156.

173. Kuhn, J. R., & Sutton, S. G. (2010). Continuous Auditing in ERP System Environments: Current State and Future Directions. Journal of Information Systems, 24(1), 91–112.
174. Singleton, T. W., & Singleton, A. J. (2010). Fraud Auditing and Forensic Accounting (4th ed.). Wiley.
175. Teeter, R. A. (2010). Remote auditing. Journal of Emerging Technologies in Accounting, 7(1), 73-88.
176. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.
177. Coderre, D. (2009). Computer Aided Fraud Prevention and Detection: A Step by Step Guide. Wiley.
178. Khan, R., Corney, M., Clark, A., & Mohay, G. (2009). A role mining inspired approach to representing user behavior in ERP systems. Proceedings of the Asia Pacific Management Conference, 14, 1-12.
179. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. Journal of Information Systems, 22(2), 195-214.
180. Curtis, M. B., & Payne, E. A. (2008). Contextual and Individual Factors That Influence Implementation Decisions for Technology Within Auditing. International Journal of Accounting Information Systems, 9(2), 104–121.
181. Dowling, C., & Leech, S. (2007). Audit support systems and decision support. International Journal of Accounting Information Systems, 8(2), 92–116.
182. Proctor, P. E., Heiser, J., & MacDonald, N. (2007). MarketScope for Segregation of Duties Controls within ERP. Gartner Research Report R2183.
183. Vaidya, J., Atluri, V., & Warner, J. (2007). The Role Mining Problem: Finding a Minimal Descriptive Set of Roles. Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, 175–184.
184. van der Aalst, W. M. P., Reijers, H. A., Weijters, A. J. M. M., van Dongen, B. F., de Medeiros, A. K. A., Song, M., & Verbeek, H. M. W. (2007). Business process mining: An industrial application. Information Systems, 32(5), 713-732.
185. Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8), 861-874.
186. Winkler, W. E. (2006). Overview of record linkage and current research directions. Bureau of the Census Research Report Series.
187. Arnold, V., Collier, P. A., Leech, S. A., & Sutton, S. G. (2004). Impact of intelligent decision aids on expert and novice decision-makers' judgments. Accounting and Finance, 44(1), 1-26.
188. Hodge, F. D., Kennedy, J. J., & Maines, L. A. (2004). Does search-facilitating technology improve the transparency of financial reporting? The Accounting Review, 79(3), 687-703.

189. Hunton, J. E., & Rose, J. M. (2004). Effects of PCAOB staff accounting bulletins on auditor judgments. Auditing: A Journal of Practice & Theory, 23(1), 1-19.
190. Krippendorff, K. (2004). Content Analysis: An Introduction to Its Methodology (2nd ed.). Sage.
191. Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1-21.
192. Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives. Managerial Auditing Journal, 18(9), 725-731.
193. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2002). Feasibility and economics of continuous assurance. Auditing: A Journal of Practice & Theory, 21(1), 125-138.
194. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.
195. Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. Auditing: A Journal of Practice & Theory, 21(1), 147-163.
196. Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process. Managerial Auditing Journal, 16(3), 152-158.
197. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5-32.
198. Elkan, C. (2001). The foundations of cost-sensitive learning. Proceedings of the 17th International Joint Conference on Artificial Intelligence, 973-978.
199. Bell, T. B., & Carcello, J. V. (2000). A decision aid for assessing the likelihood of fraudulent financial reporting. Auditing: A Journal of Practice & Theory, 19(1), 169-184.
200. Drake, P.D., & Nigrini, M.J. (2000). Computer assisted analytical procedures utilizing Benford's Law. Journal of Accounting Education, 18(2), 127-146.