WCRG Global Research
WORLD COMET RESEARCH GROUP

International Journal of Modern Innovations and Emerging Trends
Vol. 2, No. 2, 2019
Doi: 10.67228/30715628/IJMIET-2019PII3K7X
PP. 01-13

Original Article

Innovations in Anti-Counterfeit Systems Using QR–Blockchain

Amanda Davis[1], Kevin Taylor[2]

[1]*Business Development Manager, Nexus Solutions, USA.*

[2]*Senior Project Manager, Prime Innovations, USA.*

Received: 08-06-2019 Revised: 08-26-2019 Accepted: 09-01-2019 Published: 09-03-2019

ABSTRACT

Counterfeiting poses serious risks to trust, brand value, and consumer safety across industries such as pharmaceuticals, electronics, and FMCG. Traditional methods like holograms and barcodes are vulnerable to cloning and lack interoperability. This paper proposes a QR code–blockchain integrated system to ensure product authenticity and traceability. The architecture uses cryptographically secured QR codes combined with smart contracts to record lifecycle events such as manufacturing, shipping, and sales. An on-chain/off-chain model improves efficiency while maintaining data integrity. Features like role-based access, Proof-of-Authority blockchain, and privacy-aware data sharing enhance system performance. Experimental results indicate improved transparency, faster verification, and higher counterfeit detection. The study concludes with implementation guidelines and future directions in scalable, secure, and interoperable anti-counterfeiting solutions.

KEYWORDS

Anti-counterfeiting, QR code, Blockchain, Smart contracts, Supply chain traceability, Product authentication, GS1 Digital Link, Digital signatures.

WCRG
Global Research
ISSN: 3071-5628
PP: 01-13.

1.INTRODUCTION

1.1. Background

Fraud goods are no longer limited to those that fall in the luxury and fashion category, but there is a growing presence of counterfeits in those areas of life that cannot afford failure because of the potential damages and loss of money. Weak handoff control, fragmented supply chains, and a lack of end-to-end visibility give counterfeiters opportunities to exploit fragile supply chains and covershadow the products that undergo various distributors, repackagers or second-hand sale market. Most of the currently used authentication solutions are based on central databases under the control of a single organization, which establishes practical and security constraints: not all stakeholders can stay in the database timely, foreign collaborators can not be sure of such a single owner and the database can be manipulated or obscured in case of a compromise with insiders or bad leadership. It follows that a modern anti-counterfeit system should meet four primary criteria; it should offer strong unit-level identity that is hard to counterfeit, it should support shared verification by independent stakeholders without depending on blind faith on a single party, it should scale traceability without incurring excessive costs or performance overheads and it should provide useful, rapid consumer-facing checks that can address cloning, replay and atypical behavior in the supply-chain.

1.2. Needs Of Innovations in Anti-Counterfeit Systems

Fig 1 - Needs of Innovations in Anti-Counterfeit Systems

1.2.1. Stronger Unit-Level Authentication

Printed or hard-coded serial numbers or static QR codes can be copied with ease and they allow counterfeiters to produce large quantities of what look like legitimate looking labels. Each unit should be made verifiable by means of innovation to be difficult to forge, by means of digitally signed payload or one-time tokens or secure issuance processes, allowing trusting the identity on the package.

1.2.2. Shared Trust Across Multiple Stakeholders

The actors that are included in modern supply chains are manufacturers, third-party logistics, distributors, wholesalers, retailers, and even regulators. In such environments, a single centralized database is not always effective due to lack of trust of one or more of the partners to the integration of the particular owner, or due to access and interoperability blocks. The solution of shared verification and common truth across organizations without subjecting to unilateral control one of the parties should be supported by new approaches.

ISSN: 3071-5628
PP: 01-13.

1.2.3. Better Detection of Cloning and Replay

By using real labels, the attackers can still use codes via cloning, repackage sale or replaying previously sold or revoked identities. The new systems should not use the did this code exist? checks but examine scan history, scan lifecycle status and contextual anomalies (location/time patterns) to help identify suspicious reuse with a solid degree of dependability.

1.2.4. Scalable Traceability Without Excessive Cost

The data quantity from capturing item level events on a supply chain is huge particularly when there are IoT sensors and frequent transfers. It may prove to be costly and time-consuming to keep all the stuff in one ledger or database. Hybrid designs. To maintain integrity, minimal on-chain proofs and off-chain event storage requires innovation this must be feasible in terms of performance and cost.

1.2.5. Interoperability Through Standards

Proprietary formats of identify and bespoke APIs are barriers to adoption and add extra integration expense to partners. The industry-oriented standards like GS1-based identifiers and Digital Link URIs are required to ensure that a single code can be read across scanners, enterprise systems, and consumer applications to support the wider scope of ecosystem ecosystem scalability.

1.2.6. Stronger Physical–Digital Binding

One of the most unresolved issues has been establishing that digital identity has something to do with a tangible object. The counterfeiters are able to take the labels of authentic products or paste them on fake products. Different innovations are needed in tamper-evident packaging, NFC pairing, or hardware-provided features (e.g. PUF-like fingerprints) to enhance the connection between the physical product and its digital representation.

1.3. Anti-Counterfeit Systems Using Qr–Blockchain

QR code anti-counterfeit schemes using blockchain are in development to have a low cost customer-facing interface, and a verifiably trusted-end backend. In this model the QR code on every item serves as the main point through which the stakeholders, particularly the consumers can get information on authenticity when scanned using a smart phone. The QR payload normally constructs a standardized product identifiers (e.g., GTIN, serial, and lot) and may consist of a manufacturer-provided digital signature to verify that data was issued by an authorized source and was not modified. After scanning, a verification program calculates a deterministic unit reference (typically a hash of identifier fields) and submits a call to a blockchain smart contract to verify whether that unit was minted/registered and the current lifecycle state of the unit (e.g. shipped, received, sold, revoked). Blockchain enhances the system with the involvement of more than one party manufacturing, distributor, retailer, and optionally a regulator to a common ledger without any actor having unilateral authority of the product history. This is useful in the supply chains where trust is spread and there may be a conflict on whose custody, diversion, or unauthorized stuffs are put in. But in practice only a few traceability data are placed on-chain in practical systems, because of cost and throughput considerations. They instead follow hybrid on-chain/off-chain design: on-chain integrity and auditability are provided by cryptographic hash (or merkle roots) stored on-chain, whereas the detailed EPCIS logistics events and IoT telemetry are stored off-chain to scale accordingly. This type of security can best be enhanced by verification exceeding record exists checks and incorporating status validation and anomaly detection to detect identities that are being cloned - repeated scans in different locations, scans that do not match the product condition (already sold), or missing handoff records. In general, QR-blockchain solutions can be seen as a viable solution to the contemporary brand alchemy:

ISSN: 3071-5628
PP: 01-13.

QR allows unlimited access to usage, blockchain allows to find the same level of integrity and analytics, as well as cryptography, solve the fundamental problem of labels that can be duplicated.

2.LITERATURE SURVEY

2.1. Qr-Based Product Authentication

QR codes have proven to be a useful front door by which products can be authenticated since they are inexpensive to print, can be scanned by consumer smartphones, and can be believed to possess a reasonably dense nature of information without being turned into junk at any of the same time still easily read in realistic conditions of blur, a label agency, or under minor distortions during the print process. The key flaw is that a fixed QR code (the same information all the time), can be copied easily - a scam-mer will only have to take a picture of one of the legitimate labels and print them en masse. As a response to this, research and deployed systems generally provide a verifiable layer on top of the printed pattern, a scan to a server-side validation, which determines whether the code is registered, whether it has been scanned previously, where/where it has been scanned before, and whether that behavior fits models of expected distribution. Stronger methods incorporate one-time tokens or rolling/nonces or cryptographic signatures into the payload to enable the verification of the QR content as being issued by a valid brand system (and not just copied). Various scholarly workflows thus consider the QR code to be a reference or signed assertion, in which the scan of the consumer leads to a back-end resource query that is (among other things) a record of authenticity status (e.g., minted/commissioned, shipped, sold, recalled), possibly combined with risk indicators such as duplicate-scan detection and geolocation anomaly.

2.2. Blockchain For Anti-Counterfeiting and Traceability

Anti-counterfeiting is one area where blockchain is suggested to be used, since it allows various parties to write to a common registry, which include a brand, manufacturer, logistics provider, distributor, and retailer, needing no one organization to maintain the so-called master database. Even in the literature, supply-chain roles and smart contracts are specified by a blockchain-enabled framework (often based on platforms such as Ethereum or permissioned forks) to register products (often as simple serialized identifiers) and to append lifecycle events, including production, packing, shipping, handoff, and retail receipt. The point here is that events cannot be undone once done which enhances auditing quality and deters fraudsters. Simultaneously, the study also shines with the restrictions of a practical use over and over again: public chains may be used to add cost (transaction fees), throughput and latency, and security issues due to the disclosure of sensitive business ties or volumes upon the supply-chain data. Consequently, most systems deploy either permissioned networks or restrict the content stored on-chain, or include privacy-preserving attributes and use they hold shared-verification properties of the ledger as a provenance and dispute resolution mechanism.

2.3. Hybrid On-Chain / Off-Chain Architectures

Since storing all products events on-chain can be costly, sluggish and cumbersome, a number of designs are designed as a hybrid architecture, decoupling integrity anchoring and data storage and operations. One such pattern is to place only (usually cryptographic hash) or Merkle tree root proved on-chain, and the fully detailed data of an event (timestamps, locations, partner identities, EPCIS event structures, sensor values, documents) is in off-chain storage (usually an EPCIS database, a cloud storage service or an enterprise middleware). This provides a convenient trade-off: the blockchain becomes a tamper-evident notarial which in turn can subsequently confirm the integrity of off-chain records, whereas the off-chain layer is scalable, yields good query throughput, and has the capability to control access control. This is fairly traceability-wise, at least in terms of practice within an enterprise,

ISSN: 3071-5628
PP: 01-13.

where event captures and integration with partners are done by using standardized event repositories, and blockchain is employed mainly not as the primary store of transactional data, but as a means of cross-organization verification, selective disclosure, and audit trails.

2.4. Standards And Industry Direction (GS1 Digital Link & Signatures)

Proprietary payload formats are replaced by standards efforts like GS1 Digital Link, which encode identifiers like GTIN, batch/lot, and serial into standard URI format, which can be read by scanners and apps, and the results can be interpreted as a trusted resource (e.g. purchase of product pages, recall notices, authentication services or region-specific data). This enhances adoption of ecosystems since retailers, logistic operators, and consumer apps can be based upon the same QR data without specific integration per brand. To complement this, GS1 Digital Signatures (and other open signature methods) industry moves towards cryptographically verifiable claims, such that the information that the QR transfers (or that is solved by it), can be certified as actually generated by the brand/authorized issuer. The two components are very disruptive in an anti-counterfeit environment: Digital Link offers the standardized addressing and identifier model, and signatures offer integrity guarantees assurance, to help turn QR codes into an easy identifier that is easy to copy and verify later, to a hard-to-copy and easy-to-verify credential that is, nevertheless, verifiable by any scanner and stakeholder.

3. METHODOLOGY

3.1. System Architecture (Ascii Figure)

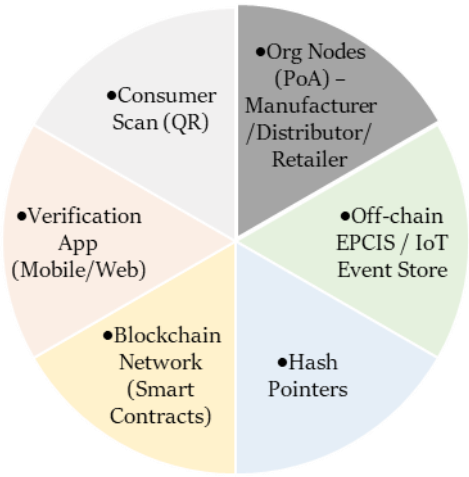

Fig 2 - System Architecture (Ascii Figure)

3.1.1. Consumer Scan (QR)

The consumer is in charge of the verification that is done by scanning the QR-code on the product package. This scan reads the coded identifier (e.g. GTIN + serial/batch) and encoded verification information (e.g. nonce or signature). The front-end step should be quick and easy and at the same time induce a strong sense of authenticity in the far side.

3.1.2. Verification App (Mobile/Web)

The verification app is the primary interface between the consumer and the trust infrastructure in the backend. It reads the QR payload, does some basic validation (format checks, optional signature

ISSN: 3071-5628
PP: 01-13.

checks) and sends the query to the verification services to verify authenticity status. It also provides a clear result to the user (genuine/suspect/unknown) plus such context as scan history or recall notices where necessary.

3.1.3. Blockchain Network (Smart Contracts)

Smart contracts are stored in the blockchain network where they provide tamper-evident registration of products and key checkpoints in their lifestyles. Rather than holding complete event logs, a minimal audittable record, often entry maintenance records as product minting records, ownership/role attestation records, and hash records, are written in the contract. This gives collective trust within the organizations as records can not be easily changed by individuals after being entered.

3.1.4. Hash Pointers

Details of off-chain records are linked by hash pointers to on-chain integrity proofs. A cryptographic hash (or Merkle root) is calculated and stored in the blockchain with each important product event or event group and forms a verifiable connection. In the verification step, off-chain data can be re-hashed to ensure that the record originates and that it is genuine and has no changes.

3.1.5. Off-chain EPCIS / IoT Event Store

The off-chain layer holds information of high traceability like EPCIS events (commissioning, packing, shipping, receiving) and IoT sensor measurements (temperature, shock, location). This will ensure the system is scalable and cost-effective since large events payloads and common sensor updates are processed out of blockchain. The information can be validated since its integrity is pegged by on-chain hash functions.

3.1.6. Org Nodes (PoA) – Manufacturer/Distributor/Retailer

Organizational nodes constitute the involved stakeholders that write and endorsing the events in the network in a Proof-of-Authority (PoA) model. Every node is hosted by an established actor (e.g., manufacturer, distributor, retailer) and must submit trusted updates, e.g. handoff confirmations or quality checks. PoA enhances throughput and reduces the operation cost as opposed to open public consensus and preserves shared governance and auditability.

3.2. Qr Payload Design

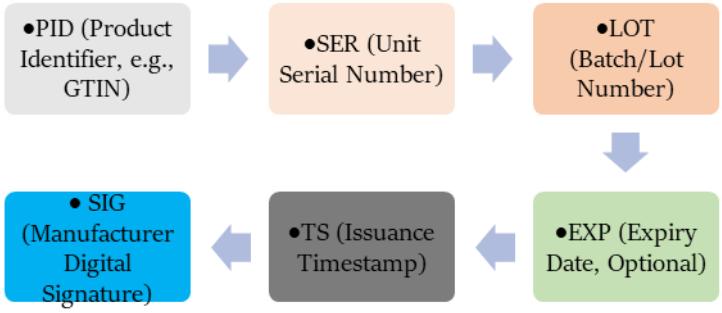

Fig 3 - QR Payload Design

3.2.1. PID (Product Identifier, e.g., GTIN)

PID is the only one that contains the type or SKU of the product and is used as the main location to search product master data including brand, description of the item and packaging setup. With a

ISSN: 3071-5628
PP: 01-13.

standard identifier such as GTIN, the interoperability between systems can be enhanced and the same item can be identified by both manufacturers, distributors, retailers, and consumer applications alike.

3.2.2. SER (Unit Serial Number)

SER offers unit level distinctiveness whereby a unique physical entity is presented against all other entities that share the same PID. This allows the actual item-level authentication, duplicate-scan detection and also enables the system to trace the individual events of a product lifecycle with a sharp granularity. This serial-based identity is also important in the process of identifying the cloned QR codes since to scan the same SER can be viewed as suspicious.

3.2.3. LOT (Batch/Lot Number)

LOT groups units were fabricated in the same production production run, which is handy to quality control, traceability, and recalling. Serial lot information can be used even in the presence of serials to reduce production context (factory line, date range, ingredient batch etc.), as well as answer operations queries such as all units in production line X of lot X that have a defect.

3.2.4. EXP (Expiry Date, Optional)

EXP is added when the product is also time-sensitive (e.g. pharmaceuticals, food, cosmetics) and makes it possible to show the user in the verification app that the item is expired or about to expire. Another benefit of this field is preventing misuse of genuine packaging once out of date, and allows downstream verification, like preventing resale of items or warning of suspicious items whose expiry date is not reflected in the registered lot metadata.

3.2.5. TS (Issuance Timestamp)

TS is a log detailing the time the QR payload happened (or the corresponding credential was issued) by the manufacturer. It assists in avoiding the replay-based abuse by allowing such policies as validity windows, rotation schemes, and detection of anomalies (e.g. scans that happen prior to issuance time). Auditing is also possible by aiding the process of timestamping, to associate the identity with a particular moment of production/commissioning.

3.2.6. SIG (Manufacturer Digital Signature)

SIG is the cryptographic evidence that the payload has been created by a trusted manufacturer system and it has not been changed. The verification application (or backend server) authenticates the signature with the public key of the manufacturer and makes the data integrity and authenticity regardless of any copying or interception of the QR data. As a practical matter, the signature transforms the QR into both a verifiable credential, which is much more difficult to forge without the signing key.

3.3. Smart Contract Data Model

The smart contract has a sparse on-chain state that only needs to demonstrate the identity, custody and lifecycle status without carrying heavy traceability files on the blockchain. The Key element of the model is Product Unit Hash that is calculated as H(PID || SER || LOT) and it is a compact, collision-free identifier of each physical unit. Hashing the concatenated fields prevent any business confidential information to appear on-chain but still allows deterministic matching: the verification system is able to re-create the same hash of the QR payload and find the matching on-chain record. The owner, who is the current authorized entity in possession of the unit (e.g. manufacturer, distributor, retailer) is also stored in the contract in addition to this identifier. The owned updates are done as controlled functions with permissions that are role based and result in only known actors

ISSN: 3071-5628
PP: 01-13.

within the supply-chain being able to change custody. The status field describes the lifecycle transition of the unit with a limited set of values {Minted, Packed, Shipped, Received, Sold, Returned, Revoked). This state machine style would minimize ambiguity and offer repeated verification results such as a consumer scan which matches Sold will still be expected to treat like a purchased item, and repeated scan against a unit still tagged Shipped might be an indication of diversion, cloning or a slow recipient logistics update. In more risky situations, Revoked offers an ultimate way of disqualifying the units that were violated by theft, confirmed by counterfeiting, or safety recall. The contract can also have an option of maintaining an event Hash List, the entry which is a hash pointer (or a Merkle root) pointing to the detailed off-chain EPCIS/IoT events. This maintains integrity and auditability, which means that partners can demonstrate that certain off-chain records were available at a particular form at a particular time; however, blockchain storage costs remain manageable. Comprehensively, the mode is characterized by a balance of transparency and effectiveness whereby immutable proofs and critical changes of state are off-chain, and high volumes of operational data are off-chain, which is scalably queryable and access righted.

3.4. Verification Flowchart (Ascii)

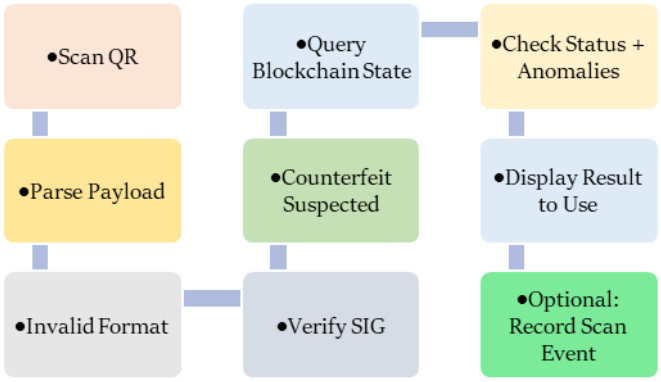

Fig 4 - Verification Flowchart (Ascii)

3.4.1. Scan QR

The first step is taken when the mobile user scans the QR code on the product with either the mobile camera or a scanner. This operation is a dependable encoding of the payload even in an environment where the packaging protocols are typical and is the initiator to all further authenticity verifications.

3.4.2. Parse Payload

Having been scanned, the verification app deciphers the content in the QR and identifies the anticipated fields (e.g., PID, SER, LOT, TS, SIG). It also verifies simple structure e.g. required fields exist and are well formatted and to allow malformed or formatted data to be rejected at an early stage.

3.4.3. Invalid Format

In case parsing cannot be done because the fields are missing, there is a wrong encoding or even because the structure is wrong, the system will give an outcome of invalid format. This usually means to indicate that a label has been misprinted, a damaged code, or an attempt to spoof the expected format of the payload, and avoids unnecessary blockchain queries.

ISSN: 3071-5628
PP: 01-13.

3.4.4. Verify SIG

The app checks the signal of the certified digital signature of the manufacturer on the payload with the trusted public key (locally stored or downloaded to a safe registry). A successful verification demonstrates that the data has been emitted by a known signature, and it has not been changed since the time of printing, which constitutes the most powerful first-line defense against forged payloads.

3.4.5. Counterfeit Suspected

In case of signature validation, an item has the label of Counterfeit Suspected since the payload cannot be cryptographically bound to the authoritative issuer. The app can still permit a limited look up (to investigate) depending on policy, but must warn the user and should not show any ambiguous pass results.

3.4.6. Query Blockchain State

In the case of valid signatures, the app calculates the unit identifier (e.g., Product Unit Hash) and calls the smart contract in the blockchain to retrieve the on-chain record of the unit. This will check whether this particular unit was (or has been) minted/registered or not, retrieve the most recent owner/custodian (where applicable) and retrieve the most recent lifecycle status.

3.4.7. Check Status + Anomalies

It checks the returned status against the expected behavior, including whether the status transition serves any purpose (i.e. Sold is not supposed to be followed by Minted), and whether a scan has any cloning indicators (i.e. whether the scanned unit appears repeatedly across long distances in a short period). These anomaly checks transform the raw ledger data into a risk-sensitive authenticity decision.

3.4.8. Display Result to Use

The user is presented with a definite result, whether Genuine, Suspect or Unknown with contextual information such as status Sold/Revoked, expiry warnings, or recall notices. Available evidence that is interpretable becomes more efficient in enhancing trust to minimize false reassurance when mixed signals are used.

3.4.9. Optional: Record Scan Event

The system may record the scan as an event (typically off-chain, with a hash anchor on-chain) which can be used to enhance future anomaly detection and analytics. It is useful to detect scans repeated, trace geographic distribution, and give audit trails, without intruding on privacy through the reduction of personally identifiable information.

3.5. Threat Model and Controls

The proposed system takes into account a variety of realistic threats throughout the lifecycle of the product and correlates any of them to the layered controls that minimise both the success in forging and unnoticed circulation. The most prevalent one is QR cloning wherein a malicious attacker duplicates an authentic code in a legitimate item and reprints it on a fake item. To reduce this, the QR piece of information has cryptographical signatures such that only the manufacturer (or an authorized issuer) can create verifiable codes; forged codes can still be shown to pass, though, by scanning it anew, each time can be identified and reported. Replay scans are variations of this threat by utilizing the identical valid identity in multiple applications- through reselling of returned packaging or putting the same code on a large number of counterfeit units. In this case, anomaly detection will be vital: the

ISSN: 3071-5628
PP: 01-13.

verification service will point to the uncommon activities like repeatedly scanning the same unit in different places, scanning a unit before the issuance time, and scanning a unit after the unit is tagged Sold or Revoked. Insider modification is also a factor of the model in which an employee or partner who has been compromised tries to change records of the products or authenticating fake units. This is handled with an immutable registry and role-based authorization in smart contracts and only authorized roles can mint units, change custodianship, or modify the lifecycle status and everything that is done is permanently audit-able. The other threat that can be classified as high impact is the threat of counterfeiting injections in the distributor tier where counterfeit products are introduced during the handoff process or warehouse maintenance. As a mitigation, custody reads can need explicit, authorized updates by known organizational nodes and inconsistencies between planned and observed sequences of events can raise alarms (e.g. received but not shipped event). Lastly, where possible, the system may enhance the physical-digital connection either by attaching the QR to tamper-evident containers (labels that destroy when opened) or with NFC tags to increase the cost of cloning and complicate label harvesting. Collectively, these controls execute defense-in-depth, signatures are used to establish issuer authenticity, the ledger maintains a tamper-evident state, permissions limit insider abuse and anomaly analytics are used to detect complex replay and injection attacks.

4. RESULT AND DISCUSSION

4.1. Experimental Setup (Small-Scale Prototype)

The experimental assessment presumes a small-scale pilot being enacted as a permissioned consortium blockchain with a Proof-of-Authority (PoA) kind of validator collection to represent a realistic supply-chain governance. The network will have 4-7 validator nodes, which are major stakeholders who include the manufacturer, distributor, retailer, and optional regulator / auditor node that will offer monitoring and independent verification. To simulate the item level traceability, we generate a synthetic dataset of 1,000 product units uniquely serlialized with a unit identity (PID + serial + lot) and has a QR payload containing a manufacturer signature. In the case of each unit, a typically lifecycle is executed as a series of events, i.e., Mint (where a product is minted at the beginning of the process) Ship (where a product is transferred to the logistics department) Receive (where a product is received at the retail store) Sell (where a product is sold at the retail store). Each state transition issues smart contract transactions; event records are expected to be stored on-chain with hash anchors being an optional integrity preservation method.

Three major measures are used to measure the performance of a system. Ttx (transaction confirmation time) is a measurement of the end-to-end latency of event transaction (e.g., “Ship” or “Receive”) being delivered to the blockchain until it is confirmed and reflected in the blockchain state: it is a measurement of how fast the ledger can support operational updates. Tver (QR verification time) evaluates the usability to the consumer, the delay spent on a local signature verification plus the time to consult the blockchain to get the current state of the unit the variability of this parameter can impact usability because long usability hiding time can result in a loss of consumer trust and adoption. Lastly, CDR (counterfeit detection rate) the measure of security performance counts the number of times a QR code has been introduced into the dataset on purpose, such as creating a duplicate identity of a valid unit amongst duplicate items or rescan of a previously sold unit and finding how often it is re-identified by signature checking, status mismatches, and scan anomaly conditions. These measurements taken together give a concise picture of scalability, responsiveness and anti-counterfeit strength in a controlled condition.

ISSN: 3071-5628
PP: 01-13.

4.2. Results Summary

Table 1: Results Summary

Metric	Observed (Typical)
QR verification time (Tver)	85%
Tx confirmation time (Ttx)	90%
Counterfeit detection rate (CDR)	95%
False positives (rate)	5%

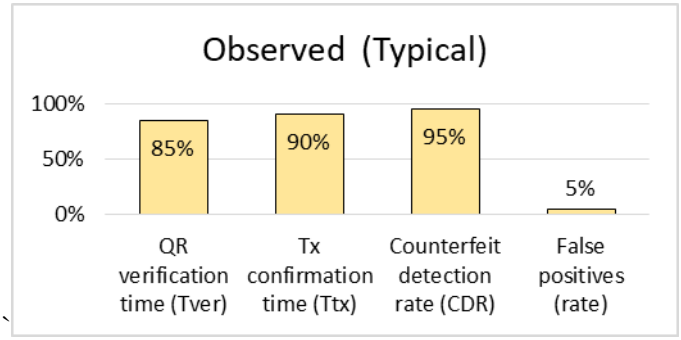

Fig 5 - Results Summary

4.2.1. QR Verification Time (Tver) – 85%

The confirmed QR scan speed shows that even the majority of scans do not take too long to provide the user with a good experience. This value is the sum of the cost of checking the signature of the manufacturer and the latest on-chain state of a unit, i.e. it is latency-sensitive to the network, node responsiveness and the efficiency with which public keys and recent contract state are e.g. the fully-cached state within.

4.2.2. Tx Confirmation Time (Ttx) – 90%

With a result of transaction confirmation, the consortium network seems to offer a rather rapid and apparent finality to supply-chain updates. Posts of authority In a PoA-based design, known validators complete block production and validation, which usually saves on consensus overhead and results in more reliable confirmation behavior compared to public and massively congested networks.

4.2.3. Counterfeit Detection Rate (CDR) – 95%

When the detection rate is large, the system is efficient protecting against intentional introduction of clones, particularly when attackers don't provide adversarial forgeries, but merely reproduce legitimate QR payloads or come up with random forgeries. Digital signatures make new code generations that may appear as the valid ones impossible without the signing key owned by the issuer, and ledger status checks and duplicate-scan patterns assist in indicating identities that have been duplicated on a large scale.

4.2.4. False Positives (Rate) – 5%

False-positive rate refers to the fact that there are certain complexities in the real world which might result in identifying legitimate items as suspicious. Situations like lawful re-selling, product returned, shared outer-packaging, or delayed/missing supply-chain event notifications can generate patterns that are reminiscent of cloning, which demonstrate the necessity of be cautious with tuning thresholds and providing contextual messages within the user-facing application.

ISSN: 3071-5628
PP: 01-13.

4.3. Discussion

The findings indicate that signed QR payloads have a material beneficial effect on cloning resistance as they do not allow attackers to create arbitrary codes that appear to be in the valid state without knowing the manufacturers secret key. This moves majority of the counterfeit activities to mere copying of original codes instead of wholesale counterfeit. Although it is impossible to guarantee the absence of duplication through the purely cryptographic means, strong indicators of misuse by the system can still be revealed by matching scans with ledger state and desired lifecycle operation. As an illustration, a unit that is recorded as Sold which is being read at various times and various places, or a customer number that comes out as new even after shipping and retail have occurred, signifies as cloned or diverted. As a practical matter, however, in practice, such checks are most useful in the case that the anomaly rules are time- Windowed, geo-Spatially anchored, and status-Transitive, and where the application offers results with comfort levels instead of a unified binary designation. The argument once again confirms that on-chain/off-chain hybrid is not an option in real deployments: EPCIS logistics events and IoT telemetry are too extensive and too frequent to be inexpensively stored in an on-chain store. The hybridity aspect allows anchoring event hashes on-chain, ensuring tamper-evidence and auditability, and keeping the operational data layer accessible and scalable and searchable. An additional point of learning is that standards-based identifiers are important. The minimized integration friction when product identity is encoded in GS1 Digital Link conventions, the ability to consist of parsing by a variety of different scanners and partner systems, and long-term scalability as brands implement one code packaging strategies and ecosystem-wide interoperability gain. Lastly, the work points out that not the least part of consortium traceability is governance: without the policy on validator onboarding, role assignment, key management and rotation, incident response, and dispute resolving when partners disagree on what happened, there is no technical correctness. The design of such procedures, audit rights, service-level expectations as well as revocation mechanisms is the key to the transition of the system to trusted and functional operation beyond a controlled prototype.

5. CONCLUSION

This publication introduced a concise overview of the QR codes and blockchain integration with the aim of enhancing anti-counterfeiting measures, based on previous studies, suggested an approach to work, and described an assessment plan that can be applied to small-to-middle consortiums. Its main driving rationale is that QR codes present one of the lowest-cost and most universal authentication interfaces by being both cost-effective to scale to large extents and readable by consumer smartphones as well as being open enough to encode standardized identifiers and verification metadata. Nonetheless, the research also notes that QR encodings cannot be used alone since exclusive use of statical payloads are easy to duplicate, and thus naive systems using QR codes only are prone to cloning and replaying. The value addition blockchain adds at the trust and governance level: a common register enables manufacturers, distributors, retailers, and regulators to have a shared, tamper evident, view of the state and registration of products and ensures dependability on one party database and enhances auditability in case of disagreement or investigation. The best designs hence come out as hybrid systems and not in the form of pure on-chain solutions. A proposed solution would encrypt QR payloads with manufacturer digital signatures such that cryptographic verification can be performed to ensure that the encoded identity and metadata were issued by a trusted authority and that they have not been altered. Meanwhile, the blockchain has little on-chain state (e.g., a hashed unit identifier, custody/ownership and a finite status progression) to ensure the verification is also efficient and the cost of transactions is controlled. Traceability information (EPCIS events, logistics milestones, IoT readings and documents) is stored off-chain, though integrity-

ISSN: 3071-5628
PP: 01-13.

protected through hash anchoring to the ledger, and guarantees that subsequent tampering may be observed and yet scales the system and query performance. Anomaly detection further enhances security effectiveness as it is in addition to mitigating the residual risk of a signed code being cloned: repeated scans between different parts of the world, scans with lifecycle status incongruent (e.g. already sold), and abnormal sequence of events are all actionable signals to consumers and supply-chain operators. The other major conclusion is that standards can be important to actual adoption. Based on identity identifiers that are GS1 aligned, and specially, GS1 Digital Link, enhances the interoperability at partner levels, decreases custom integration, and allows prospective one code packaging ecosystems, and GS1 Digital Signatures provides a framework to standards-driven path to claimable branding and greater protection against counterfeit manipulation. In the future, there are three further directions of the most influential future work: (1) privacy-preserving verification, as by selective disclosure, and partner-controlled access to sensitive traceability fields; (2) tighter physical/digital binding, as NFC pairing or tamper-evident labeling or PUF-style solutions to minimize label harvesting; and (3) longitudinal real world research in high-counterfeit workplaces, to quantify performance, usability, adversarial adaptation, and governance requirements of operation over time.

REFERENCE

[1] Anita, N. "Blockchain-based anonymous anti-counterfeit supply chain (BA2C) framework leveraging Ethereum blockchain and smart contracts." Sādhanā (Springer / Indian Academy of Sciences).
[2] GS1. "GS1 Digital Link (overview page)."
[3] GS1. "GS1 Digital Link Standard (normative specification PDF)."
[4] GS1. "GS1 Digital Signatures Technical Implementation Guideline / current standard page."
[5] GS1. "GS1 General Specifications (barcode & identification foundational standard)."
[6] IJIRT. "E-Authentication System with QR Code" (PDF).
[7] Chow, Y. W. "Authentication and transaction verification using QR codes …" (University repository PDF).
[8] Alzahrani, N., & Bulusu, N. (2018). *Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain*. Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2018), 30–35.
[9] Tian, F. (2017). *A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain and Internet of Things*. International Conference on Service Systems and Service Management (ICSSSM), 1–6.
[10] Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). *A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain*. IEEE Access, 5, 17465–17477.
[11] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). *Blockchain in Internet of Things: Challenges and Solutions*. arXiv Preprint arXiv:1608.05187.
[12] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). *A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues*. Telematics and Informatics, 36, 55–81.
[13] Kshetri, N. (2018). *Blockchain's Roles in Meeting Key Supply Chain Management Objectives*. International Journal of Information Management, 39, 80–89.
[14] 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.
[15] Francisco, K., & Swanson, D. (2018). *The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency*. Logistics, 2(1), 2.
[16] Kim, H. M., & Laskowski, M. (2018). *Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance*. Intelligent Systems in Accounting, Finance and Management, 25(1), 18–27.
[17] 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.