ESTABLISHING A LEGALLY DEFENSIBLE BLOCKCHAIN CHAIN OF CUSTODY TECHNICAL FRAMEWORK

by

HARRY ROBERTSON

A THESIS

Presented to the Department of Computer Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science

December 2025

An Abstract of the Thesis of

Harry Robertson for the degree of Bachelor of Science
in the Department of Computer Science to be taken December 2024

Title: Establishing A Legally Defensible Blockchain
Chain Of Custody Technical Framework

Approved: *Professor Jun Li, Director Center for Cyber Security and Privacy*
Primary Thesis Advisor

Blockchain technology offers significant potential for improving chain of custody procedures through immutable recordkeeping and transparent audit trails. However, existing research prioritizes technical innovation over legal compliance, proposing sophisticated systems without analyzing whether courts would admit blockchain-based custody records as evidence. This gap creates a fundamental barrier to practical adoption.

This thesis establishes a legal baseline for blockchain chain of custody systems by analyzing Federal Rules of Evidence, expert testimony standards (Daubert and Frye), NIST guidelines, and relevant case law. The analysis reveals that legal admissibility depends less on technical sophistication than on demonstrable compliance with established standards. Systems incorporating novel cryptographic techniques and sophisticated softwares face higher evidentiary burdens under Daubert and Frye, while systems built from well-established components – SHA-256 hashing, RSA signatures, and Practical Byzantine Fault Tolerance consensus – can satisfy authentication requirements with minimal legal risk.

This thesis presents a reference architecture that prioritizes legal defensibility over technical optimization, providing a foundation for future research. By deriving technical requirements from legal constraints rather than retrofitting legal justifications onto existing designs, this framework enables evaluation of whether proposed innovations enhance or compromise admissibility prospects. This legal baseline establishes minimum requirements that reduce evidentiary risk and provide a defensible starting point for pilot implementations that can accelerate practical adoption.

Acknowledgements

This thesis was only possible due to significant, ongoing support from Dr. Jun Li, Professor Michael Moffitt, my parents, my roommates and friends, and my girlfriend.

Table of Contents

1 Introduction

Without a legal framework establishing minimum requirements for admissibility, blockchain chain of custody research operates in a vacuum. Researchers propose optimizations and innovations without knowing which technical choices increase or decrease the likelihood of judicial acceptance. Systems incorporating unproven technologies face higher evidentiary hurdles, requiring expert testimony that may be rejected under standards like Daubert or Frye [1]. Meanwhile, simpler systems using established technologies could satisfy legal requirements with minimal testimony, creating a foundation upon which more sophisticated systems might later be built.

This thesis establishes a legal baseline for blockchain chain of custody systems – a set of minimum requirements that maximize the probability of admissibility in U.S. courts, particularly for chain of custody of digital evidence (commonly referred to as Electronically Stored Information or ESI). Rather than guaranteeing adoption, this framework identifies design choices that align with existing evidentiary law, reducing legal risk and providing a defensible starting point for future implementations. By grounding technical decisions in legal requirements, this baseline enables researchers and practitioners to evaluate whether proposed innovations enhance or compromise a system's likelihood of judicial acceptance.

After providing technical background on blockchain and chain of custody procedures, this paper reviews existing blockchain chain of custody research to identify a consistent gap: technical sophistication without legal analysis. A parallel legal review examines Federal Rules of Evidence, NIST standards, expert testimony requirements under Daubert and Frye, and recent scholarship on blockchain evidence admissibility. These technical and legal analyses converge to create a set of design principles that prioritize legal defensibility. Finally, the paper proposes a reference architecture that satisfies evidentiary requirements while avoiding unnecessary complexity that would hinder adoption.

The reference architecture is not presented as an optimal or final solution, but rather as a legally defensible foundation. Future research can build upon this baseline by proposing innovations and measuring their impact on both technical performance and legal admissibility. Some enhancements may improve efficiency without compromising legal standing; others may offer performance gains that justify accepting additional evidentiary burden. Without this baseline, however, the field lacks a reference point for evaluating such trade-offs. This approach represents a methodological shift in blockchain chain of custody research. By analyzing legal constraints first, then deriving technical requirements, this thesis reverses the current, stalled research process.

By establishing this legal baseline, this thesis aims to accelerate practical adoption. Pilot programs can begin with legally defensible systems, generating case law and empirical data that inform future iterations. As courts become familiar with blockchain chain of custody through these initial implementations, judicial tolerance for technical sophistication may increase, creating space for the innovations that current research proposes. The baseline thus serves as a foundation upon which more advanced architectures can be constructed.

2 Background

2.1 Chain of Custody

Federal Evidence Rule 901(a) states “to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is” [2]. Chain of custody provides a detailed account of a given piece of evidence as it moves between parties, guaranteeing its veracity if and when it is presented at trial [3]. For instance, after DNA evidence is initially collected by law enforcement, it must then be sent to a forensic lab to be examined, then to prosecution to be used at trial. Each of these transactions must be documented to maintain verifiable authenticity of the evidence [2].

To maintain this trail, Federal Evidence Rule 901(b)(4) presents examples of evidence that satisfy identifying evidence, including, but not limited to “Distinctive Characteristics and the Like” [2]. This category is defined as “The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.” In the case of physical evidence, this may be the serial number printed on a device, or items with inherently distinctive qualities. For digital evidence, hashes are generated to indicate the uniqueness of a particular piece of data. If the hash is altered, then the authenticity of the evidence may be questioned, or the evidence itself may be deemed inadmissible [2].

Violations of chain of custody procedure may result in mistrial, dismissal, or an overturning of a conviction if the infringement is deemed significant enough [4]. For instance, *Brady* violations [5] – the negligent or malicious withholding of exculpatory evidence from a defendant – have been the source of numerous convictions of innocent individuals [6] . Augmenting this process with blockchain may be able to stop a proportion of these convictions, as well as increase confidence in the security of chain of custody records.

2.2 Blockchain Technology

Blockchain is a distributed ledger technology that creates tamper-proof records by way of cryptographic linking and decentralization [7]. Unlike traditional databases, maintained through a central authority or singular server, blockchains are kept across numerous, often independent, computers called "nodes." Each node retains an identical record of the blockchain's entire transaction history, relying upon cryptographic validation schemes to maintain a consistent, agreed-upon state across the entire blockchain network.

The term "blockchain" is derived from its data structure. "Blocks" act as containers and store transaction data [7]. Each new block is "chained" to the previous block via cryptographic linking. These links are maintained through a data structure known as a Merkle Tree [7], which provides an algorithmically efficient way to track hash-based changes. Any attempt to alter a block will disrupt the congruency of the Merkle Tree, and become immediately invalid. Thus, blockchain is immutable: Transactions cannot be reverted or altered following their initial submission.

Blockchain achieves this immutability through cryptographic hash functions. A hash function takes data of any size and produces a fixed-length output – sometimes referred to as a "fingerprint" due to its uniqueness – that can be subsequently used to identify the data [7]. If even a single bit of the original data is altered, the hash function will produce an entirely unique fingerprint. Hashing is used in both blockchain and computer forensics to provide cryptographic security.

Each block in a blockchain contains three key elements: (1) The transaction data. In the Bitcoin blockchain, for example, a block contains numerous transactions indicating which users transferred bitcoin, how much bitcoin was transferred, and to whom the transfer was sent to; (2) the block's own hash. This hash acts as a unique identifier for the block; (3) the previous block's hash. These three elements are used to track changes to blocks, among other uses. For example, if a malicious user attempted to alter the transaction data present in Block 50 (and was able to avoid all other security protocols present on a blockchain network – an incredibly unlikely feat), the hash of the block would change. Block 51 would then notice that the previous block's hash does not reflect its own stored hash of the previous block. The attacker could then attempt to alter the previous block data stored on Block 51, but that alteration would change Block 51's hash, notifying Block 52 of an inaccuracy. The attacker would then need to recalculate every subsequent block – a task which becomes computationally infeasible as the blockchain grows.

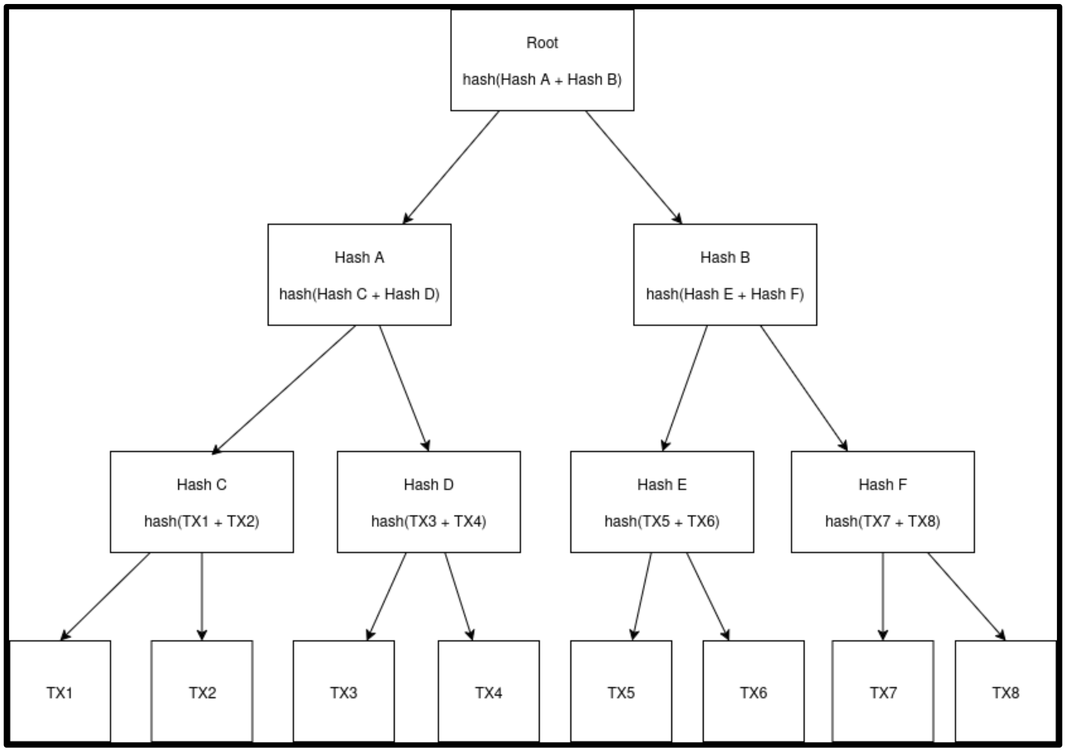

Figure 2.2.1: Merkle Tree

Because blockchain is distributed across many independent nodes, the system needs a mechanism to ensure all nodes agree on the transaction history—called a "consensus mechanism." When a new transaction is proposed, nodes must collectively validate it before adding it to the blockchain.

Different blockchains use different consensus mechanisms: In Proof-of-Work (PoW) nodes compete to solve computationally difficult mathematical puzzles. The first node to solve the puzzle gets to add the next block and is rewarded. This is the consensus mechanism used by Bitcoin. The computational difficulty makes it extremely expensive to attack the network – an attacker would need to control more computing power than all honest nodes combined. Proof-of-Stake (PoS) selects nodes to validate blocks based on how much cryptocurrency they have "staked" (used as collateral). Malicious behavior results in losing the stake. Ethereum transitioned to PoS in 2022. This is more energy-efficient than PoW but creates different security considerations. For example, a user with an excessive stake gets increased control over validation. In certain circumstances, this over-centralizes the network and leaves the network more vulnerable to attacks by that staked user. This is offset, though, by the risk associated with a greater stake. Practical Byzantine Fault Tolerance (PBFT) is a voting-based mechanism where designated nodes vote on transaction validity. This is faster but more centralized, typically used in permissioned (private) blockchains [7].

For a chain of custody application, the consensus mechanism determines how custody transfers are validated and recorded. A system using PoW would require significant computational resources; a system using PBFT would require trusted validator nodes (e.g., designated court administrators).

Blockchains can require varying levels of access. The most culturally prominent blockchains are permissionless and public. These blockchains rely upon the robust, trustless cryptographic protocols used by blockchains to ensure that malicious actors cannot take control of the network. That said, a public blockchain still incurs the risk of compromisation. Private, permissioned blockchains require prior authorization to participate in the blockchain. In a chain of custody context, a private blockchain better fits the design requirements presented. On a public blockchain, sensitive evidence is at a greater risk of being exposed to non-authorized participants. In certain instances, this could jeopardize a case.

2.3 Smart Contracts

Some blockchains, particularly Ethereum, support "smart contracts" – self-executing programs stored on the blockchain [8]. When predefined conditions are met, the smart contract automatically executes without human intervention. Smart contracts allow for the production of decentralized applications, like chain of custody operations.

For example, a smart contract for chain of custody might specify: "IF Officer X is authorized, SUBMIT evidence_record to blockchain. ELSE REJECT submission." This logic executes automatically and immutably records the result on the blockchain. On the Ethereum blockchain, the cost to execute a contract scales with its computational complexity: If a contract contains dynamic, multi-phased code with complex operations, it will require more currency to execute.

Smart contracts are written in programming languages and compiled into bytecode that runs on the blockchain's virtual machine. Once deployed, the contract's code cannot be altered. This immutability can be problematic if bugs are discovered [8].

2.4 Blockchain and Chain of Custody

Blockchain's properties align remarkably well with chain of custody requirements. Immutability, the quality that prevents retroactive changes to the blockchain, adds another layer of security against evidence tampering. Traditional databases retain the potential for malicious actors to compromise and alter evidence.

Blockchain's distributed nature complements the decentralized structure of the United States justice system [9]. The many different jurisdictions and layers that comprise the justice system provide a foundation for the distribution of nodes. Furthermore, the legal system, marred by an adversarial standard of engagement that foments procedural inequality, would greatly benefit from the introduction of a system that denies disproportionate control to any one party (defense attorney, prosecution, law enforcement, etc.) [9].

Many of blockchain's cryptographic protocols are in agreement with existing NIST standards for digital evidence preservation and evidentiary statutes [11]. The NIST requests comprehensive timestamping and logging associated with each piece of evidence entered into chain of custody. These procedures are inherent to blockchain's functionality.

Despite these numerous congruencies, the steps to practical adoption are far from simple. Immutability, although a boon for secure recordkeeping, presents unique legal challenges when confronted with destruction orders [12] or inadvertent disclosures [13]. Furthermore, many technical hurdles impinge blockchain's efficiency in a courtroom context, including storage costs [14], the "garbage in, garbage out" paradigm [15] (discussed further in section 6), and secure networking [11]. Any blockchain chain of custody design must optimize for these difficulties.

3 Technical Literature Review

Existing research demonstrates significant technical innovation while systemically neglecting the legal compliance necessary for practical adoption. These studies leave a critical gap wherein researchers continually optimize their systems without establishing a legally defensible baseline from which they can defend their system's legal reputability. Without such a baseline, the odds of eventual adoption decrease, with increased complexity diminishing the probability of future pilot programs or widespread acceptance in the scientific community.

3.1 Technological Contributions Without Legal Grounding

"Forensic-Chain: Blockchain Based Digital Forensics Chain of Custody with PoC in Hyperledger Composer," by Lone & Mir [16], provides a proof of concept for a modular chain of custody blockchain architecture implemented using Hyperledger Composer. The implementation provides granular, fine-tuned access control mechanisms and desirable throughput and latency metrics [16]. Furthermore, evidence items are defined as a low-overhead data structure that does not expose any actual data to the blockchain. Lone & Mir provide a technically-competent design for a blockchain chain of custody architecture. However, the legal background is murky. The paper makes no reference to: (a) Under which court or legal context the system operates under; (b) whether the system satisfies the evidentiary standards put forth by either Daubert or Frye (especially in reference to the novel addition of HyperLedger Composer), or; (c) how the system guarantees authentication of evidence as required by FRE 901 [2].

The technical implementation may be sound, but without legal grounding, it cannot be assumed that the system would survive legal scrutiny and be employed for practical use. The system's increased sophistication demands justification for whether or not expert testimony would be required [1].

"CustodyChain Guardian: Blockchain Chain of Custody Digital Evidence Preservation System," by Salih & Ibrahim [17] outlines a complex, four-layered framework meant for maximizing reliability in digital chain of custody practices. Despite rigorous design, the paper makes no reference to NIST standards, FRE statutes, or a specific governing body. Like Lone & Mir, the complexity of Salih & Ibrahim's framework is subject to scrutiny under both Daubert and Frye [1]. Again, the paper lacks a sufficient legal basis behind its innovations. It fails to address the same legal questions also omitted by Lone & Mir.

"B-CoC : A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics" by Bonomi, et al. [18] provides insights into scalability and throughput optimizations. Using Practical Byzantine Fault-Tolerance, Bonomi et al. demonstrated that storage scalability is manageable, even at a high volume. The paper found that with the submission of 100,000 "evidence items" (a bespoke data structure associated with each blockchain entry), the blockchain grows at a rate of 488 megabytes (MB) a year, including header data. Even at high volumes, defined as 1,000,000 evidence items, their implementation only consumed 3.1GB of storage space, annually [18]. These statistics were achieved through fine-tuning the block generation rate to five minutes per block.

In a practical setting, the growth rate would likely be much higher, given the large number of criminal cases tried annually in the United States. State courts alone adjudicated 66 million cases in 2024 [19]. Though sentencing data regarding these trials is not available, federal courts delivered over 60,000 convictions in the same timespan [19]. Given that evidence is *required* for conviction, the volume of evidence that a federal blockchain system would interact with would likely be considered a “high” volume, with state courts accruing significantly more data. Regardless, the storage scheme is feasible, with additional optimizations possible at the infrastructure level.

Bonomi, et al.’s proposed large-scale infrastructural design presents a viable possibility for use in the United States. Nodes are distributed across different regions, with regional governments acting as the custodian for a cluster of nodes [18]. The United States’ inherently decentralized justice system – spread across different circuits, states, and municipalities – provides the opportunity for many different governing entities to maintain a more decentralized blockchain system [9]. In this way, a system in the United States could escape risks of over-centralization.

Several other papers introduce even more complex schemes with the same facile legal analysis: “Block-DEF: A Secure Digital Evidence Framework Using Blockchain” by Tian, et al. [20] introduces a bespoke blockchain implementation that uses Named-Based Optimized Practical Byzantine Fault Tolerance, a novel consensus mechanism that assigns unique content names to each evidence file. Name-Based Byzantine Practical Fault Tolerance was designed specifically for Tian, et al.’s implementation [20]. “Blockchain-based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management” by Ahmad, et al. [21] uses blockchain-secured smart-locks to physically secure evidence, while simultaneously storing evidentiary metadata on-chain. The use of blockchain across both digital and physical evidence storage introduces additional testing requirements and complexity, both of which damage the system’s reputation in a legal setting [2].

A system using novel consensus mechanisms may outperform one using standard protocols on every technical metric – throughput, latency, security – yet face inadmissibility under Daubert or Frye if expert testimony about the novel mechanisms cannot satisfy reliability standards [2]. Conversely, a technically modest system using well-established components might achieve immediate admissibility through straightforward expert testimony and greater leniency from trial judges.

It may be the case that under legal scrutiny these systems remain compliant, however, these advancements mean little without a measurable plan for deployment and pilot programs. In essence, complexity decreases the *likelihood* of adoption under legal standards (which will be discussed further in sections 4 and 5).

Section 7 provides a comprehensive legal analysis of these papers, underscoring which aspects may be of use in a deployable system in the United States. From there, a reference architecture will be introduced defining a high-level approach to a legally comprehensive blockchain chain of custody system.

4 Legal Background and Analysis

Blockchain-based chain of custody systems must navigate a complex landscape of evidentiary standards, federal regulations, and judicial precedents. Blockchain's admissibility relies upon numerous criteria: expert testimony requirements under Daubert or Frye [2], compliance with the Federal Rules of Evidence [1] [5], adherence to the NIST evidence preservation guidelines [11], and agreement with extraneous judicial orders that affect evidence handling. This section provides an explanation for each guideline, as well as their impact on blockchain chain of custody systems.

4.1 Federal Rules of Evidence and Blockchain Admissibility

Under Federal Evidence Rule 901 [2], evidence must be authenticated to demonstrate its validity. Chain of custody is often one facet of this authentication. Digital evidence relies upon generating a hash of collected data at its provenance, and tracking that hash until its presentation in court. Physical evidence requires detailed documentation, as well as "identifying characteristics," such as serial numbers on a weapon, or other distinctive markings [2]. Blockchain has the ability to preserve and track changes to an associated evidence item through linking a record to a database entry. If the hash is altered at any point through the evidence's lifecycle, the blockchain would keep an immutable record of that alteration. This efficient tracking of hashed data also fulfills Federal Evidence Rule 902 (14) [22], which provides guidelines permitting the self-authentication of digital evidence based on – generally – the curation of uniquely-identifying hashes.

The best evidence rule (FRE 1001-1002) [23] requires that the original document, rather than a copy, be produced to prove its contents. Blockchain records satisfy this requirement because the blockchain entry itself constitutes the 'original' under FRE 1001(d) – it is the first permanent form in which custody information is recorded. Unlike a photograph of a document or a copy of a file, a blockchain record is not derivative; it is the authoritative source of the custody data it contains.

4.2 The Daubert Standard for Expert Testimony

The Daubert standard permits trial court judges to “assess the reliability and relevance of an expert witness testimony before it is presented to a jury” [1]. In 2000, FRE 702 was amended in reaction to *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) [24]. Daubert refers to the methodological validity of the expert’s presentation, as well as the validity of the field upon which they are testifying [1]. Methodological validity is determined by the presence of known error rates and widespread scientific consensus [1]. The Daubert standard supplanted the Frye standard [25] across all federal circuits and most states. Frye relied more heavily upon “general acceptance” in a given scientific field, a definition whose ambiguity caused confusion in rulings. The Daubert Standard considers five factors in determining whether an expert witness’ methodology is valid: “1. Whether or not the technique or theory in question can be, and has been tested; 2. Whether it has been subjected to publication and peer review; 3. Its known potential error rate; 4. The existence and maintenance of standards controlling its operation; and 5. Whether it has attracted widespread acceptance within a relevant scientific community” [2].

Composed of “primitives” from both computer science and cryptography [7], blockchain would likely meet the Daubert standard. For instance, the cryptography underlying blockchain’s digital signature protocol possesses methodological validity, as do commonly-used consensus mechanisms like proof-of-work and proof-of-stake [7]. Though incremental improvement of blockchain systems is undoubtedly warranted in the pursuit of a blockchain chain of custody architecture, the technology must be ubiquitous enough such to permit testimony on its behalf. Initial systems ought to focus on maintaining methodological veracity while meeting the minimum requirements for operability.

4.3 The Frye Standard

The Daubert standard largely replaced the Frye standard following *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) [2]. Daubert is active in all federal courts and the majority of states [26]. That said, California and New York, two of the most populous states in the U.S., rely upon Frye in determining the admissibility of expert testimony.

The Frye standard relies upon "general acceptance" from a scientific field to determine the admissibility of an expert opinion or evidence. In certain instances, Frye can be more restrictive than Daubert. In *United States v. Frye* (1923), courts ruled that admissibility relies upon whether or not a given scientific principle "sufficiently established to have gained general acceptance in the particular field in which it belongs" [24]. Certainly, it would be more difficult for a state-of-the-art blockchain chain of custody framework to be adopted by the courts under Frye, given that many of the components presented in the literature review have not yet gained "widespread acceptance" in the field.

The differences between Daubert and Frye highlight the shortcomings of the previously presented research: Systems may be deemed admissible in one jurisdiction and inadmissible in another [2] [24]. Because the literature provided in Section 3 [16] [17] [18] [19] does not defer to either standard, they cannot reasonably assume that their systems would be functional in the United States.

4.4 Judicial Orders and Extraneous Exceptions

In *United States v. Comprehensive Drug Testing, Inc. (2013)* [12], the court held that records obtained by the government must be "returned or destroyed." Though this is an uncommon occurrence, this would jeopardize any on-chain storage architecture.

18 U.S. Code § 3509 [27] specifies that depositions related to instances of child exploitation, abuse, or sexual abuse must be destroyed five years after the date that the court entered its judgement. If the deposition's data were to enter a blockchain chain of custody, the exposure of these sensitive materials would never be removed from the blockchain [7].

Though rare, these destruction orders necessarily preclude an on-chain blockchain storage architecture. It is true that such an architecture could persist while omitting illegal materials, however to do so would introduce additional risk in the form of accidental submissions, as well as substantial cost increases. Technical burdens such as the monetary rate of storage and scalability [14], which will be further discussed, make on-chain storage an non-viable mechanism of data preservation.

4.5 Inadvertent Disclosure

Blockchain's immutability creates unique challenges in the context of inadvertent disclosure of privileged materials. Federal Rule of Evidence 502 [28] governs the inadvertent disclosure of attorney-client privileged communications and attorney work product, establishing procedures for "clawback" when such materials are accidentally produced during discovery or evidence handling.

Under FRE 502(b), inadvertent disclosure does not waive privilege if three conditions are met: (1) the disclosure was inadvertent, (2) the holder of the privilege took reasonable steps to prevent disclosure, and (3) the holder promptly took reasonable steps to rectify the error [28]. When these conditions are satisfied, the receiving party must return, sequester, or destroy the privileged information and may not use or disclose it.

This clawback mechanism assumes that disclosed materials can be retrieved and removed from circulation – an assumption fundamentally incompatible with blockchain immutability [7]. If privileged materials or their detailed descriptions were stored directly on a blockchain, inadvertent disclosure would become permanent. Even if all parties agreed to disregard the materials, the blockchain record would persist indefinitely, accessible to any party with network access and potentially discoverable in future proceedings [7].

This tension reinforces the necessity of off-chain evidence storage. By maintaining only metadata on the blockchain rather than the evidence content itself, the system allows privileged materials to be returned or destroyed per FRE 502 [28] while preserving the custody documentation. The blockchain record would show that evidence item X was collected, transferred to forensic analysis, and subsequently returned to the producing party under a clawback order, without the blockchain itself containing the privileged content.

4.6 Chain of Custody Guidelines

National Institute of Standards and Technology (NIST) IR 8387 [11] defines the recommended parameters for the preservation of digital evidence. Specifically, digital images and files should be accompanied by “a. Documentation of the original source of the image or file and how it was created by or transferred to law enforcement. b. [NIST approved] Hashes and digital signatures… If a hash is not made, a copy of the data – created early in the collection process and preferably before any investigative procedures have begun – should be stored on physical media, and all of the transfers should be documented… Evidence files should be kept in a system that is not connected to the internet and that has strong security including individual authentication, access controls, and logging. If the organization uses a cloud-based system, appropriate security is needed. Techniques such as VPNs can be used to protect forensic evidence even while using the internet.”

These parameters greatly inform the system design of blockchain chain of custody systems. Public blockchains, like the architecture proposed by Bonomi, Casini & Cicotelli, expose data to a public network. This would violate NIST standards and limit the possibility of practical adoption. NIST 8387 provides guidelines for secure cloud storage, including, but not limited to, encrypting stored data and maintaining a plan of action for transitioning data off of the cloud in the event of disruption.

5 Legal Literature Review

5.1 Wang et al. and Blockchain Hearsay Exceptions

"Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes" by Wang, et al. (2024) [15] analyzes the admissibility of blockchain records as evidence. The authors analyze rulings on technologies analogous to blockchain, such as procedurally generated satellite images, to determine the legality of blockchain records. The paper also expands on the court's disposition towards blockchain records, broadly.

The authors make a critical distinction between machine-originated and human-originated content on blockchain. Purely automated blockchain records – transaction records, timestamps, hash values – are not "statements" under FRE 801(a) [29] because they lack human assertion. Citing *United States v. Lizzaraga-Tirado* (2015) [30], they defer to the 9th Circuit's judgement that procedurally-generated records (in the case of the ruling, Google Earth satellite images) do not constitute hearsay.

Contrarily, human-originated annotations or descriptions appended to a blockchain record would likely require a hearsay objection – most likely FRE 803 (6) [31], the "business records" exemption or 803 (8), the "public record exception" (if the system is maintained by a government entity).

Wang et al. goes on to state that FRE 902 [22], which governs self-authenticating digital records, has potential to include blockchain records as well. However, Wang, et al. fails to mention that blockchain would likely require testimony on behalf of the veracity of a given system [15]. In traditional forensics, experts are often summoned to testify as to the process by which they collected and preserved data [32]. Even in states that permit self-authentication through digital hashing, nuanced details regarding the lifecycle of the digital evidence must still be accounted for.

The paper accounts for negative attitudes towards inherent qualities of the blockchain. For example, if evidence enters the blockchain in an altered state, then the assumed reliability of the records can be detrimental to legal proceedings. Furthermore, there is a reliable way to assert that evidence entering the blockchain is inherently reliable. Wang, et al. describes this phenomenon as "garbage in, garbage out." This argument is non-unique, though, given that any evidence tampered with prior to entry into a traditional chain of custody system suffers from the same deficiencies.

Wang et al.'s granular analysis of the legality of blockchain evidence contributes to this thesis' larger discussion surrounding the legality of a blockchain evidence system. Wang, et al. establishes that individual records, if produced reliably, likely escape hearsay violations [15]. Furthermore, it establishes a set of standards for consistent blockchain admissibility, requiring a "robust consensus mechanism with the hash algorithm as its cornerstone." This outline provides additional context for establishing a functional chain of custody system.

5.2 Knight and Statutory Resolutions

"Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility under the Federal Rules" (2019) [33] by Emily Knight reiterates many of the same claims made by Wang, et al. Like Wang, et al., Knight focuses on the admissibility of blockchain evidence rather than the viability of an evidence system. Rather than adapt blockchain to fit the incongruent Federal Rules of Evidence, Knight argues that the FRE and Federal Rules of Civil Procedure be amended to accommodate blockchain [33]. Through this approach, blockchain's benefits can be entirely realized without being hamstrung by procedural quirks.

Knight notes that public blockchains lack the access control necessary to permit authentication, noting that a trusted authority is needed to correlate addresses to individuals. Knight also references Ethereum's notorious 2016 "DAO" hack [34], where attackers stole millions of dollars after exploiting faulty smart contract code. These vulnerabilities underscore the public blockchain proposal put forth by Bomoni, et al. [18]. The potential for failure is far too great to justify the increased transparency provided by a public blockchain.

Both legal analyses propose different solutions for blockchain's legal incongruencies: Wang, et al. suggests that a new system be designed around Federal Evidence Rules, emphasizing the need for trusted hashing algorithms and procedural generation; Knight notes that bespoke system designs are possible, but suggests alterations to statutes and Federal Evidence Rules provide a more streamlined path to the use of blockchain in criminal court.

6. Legal Analysis of Presented Systems

Section 6 provides a legal analysis of the papers presented in the technical review section. With a renewed perspective on the legal implications of blockchain chain of custody systems, we can use effective aspects of each system to inform our reference architecture.

6.1 Bonomi, et al.

Bonomi, et al. [18] presents the most legally viable implementation of the papers presented. The separation of on and off-chain storage, alongside the use of *Geth* – a now-deprecated Ethereum-based EVM – to deploy a permissioned blockchain, offers a generally accepted architecture that would be simple to deploy for testing purposes. The distribution of nodes across different jurisdictions offers a high-level infrastructure design that may be repeatable in the United States. Furthermore, the use of Practical Byzantine Fault Tolerance – an extensively researched, permissioned consensus mechanism – gives greater credence to the system's viability under Daubert or Frye.

Unfortunately, Bonomi, et al. proposes a public blockchain for expressly different purposes than a court would require. As discussed in Knight [33], public blockchains increase unsustainable levels of risk that could compromise sensitive criminal proceedings. That said, their architecture could be easily adapted to accommodate a permissioned system.

6.2 Lone & Mir

Lone & Mir [16] possesses many of the same architectural advantages as Bonomi, et al. Particularly, their use of an anchored blockchain reduces the chances of exposure of sensitive materials, while retaining the ability to comply with destruction orders under U.S.C. § 3509, or in cases like *Comprehensive Drug Testing* [12].

Unfortunately, HyperLedger Composer presents additional complexity that may diminish its adoptability under Daubert or Frye. Aside from its novelty, the tool has been moved to EOL (end-of-life) status and will be unable to support such a system in the future.

6.3 Salih & Ibrahim

Salih & Ibrahim [17] introduces a four-tiered framework that emphasizes minimal coupling to prevent widespread system failures. This architecture could be useful in the context of a larger, verified system. However, its innovations do not account for the initial barriers that must be overcome to achieve legal validity. As mentioned in Section 4, the paper makes no deference to legal authority, making its statutory standing murky.

6.4 Tian, et al.

Tian et al. 's [20] use of Name-Based Practical Byzantine Fault Tolerance, a custom consensus mechanism with granular access control, introduces a glaring incongruence with both Daubert and Frye. The consensus mechanism exists only within the context of this paper, and would likely require significantly more testing before its adoption. Once again, initial testing requires simpler methodologies for legitimate consideration.

6.5 Ahmand, et al.

Ahmad, et al. [21] extends blockchain protections to physical locks, relying upon its cryptographic protocols to preserve role-based access controls to physical evidence. The paper retains a digital, blockchain chain of custody repository similar to the ones presented in the previous articles, too. As a whole, the multifaceted nature of the system would require more testing than the other architectures presented. Its complexity precludes it from consideration more than a system focusing on simplistic, digital representations of blockchain chain of custody.

6.6 Synopsis

In conclusion, Bonomi, et al. [18] establishes the most legally viable blockchain chain of custody architecture. Its separation of blockchain records from physical storage, well-defined node distributions, and utilization of well-known components make it both technically optimized and legally justifiable.

Other publications introduce unneeded complexity beyond the scope of an early-iteration blockchain chain of custody system, which would be needed to establish both consensus and gather empirical data [2] [25].

7. Reference Architecture for Legal Compliance

This section introduces a reference architecture whose structure is derived from the viable components of the previously introduced papers, as well as the legal constraints defined in Section 4. These constraints reflect current judicial attitudes toward blockchain technology and its components. While courts may become more receptive to technical sophistication over time, that tolerance can only develop through initial adoption of minimally-viable, legally defensible solutions. As established in Section 6, this reference architecture prioritizes increasing the likelihood of judicial acceptance rather than maximizing technical performance or innovation.

7.1 Legal Constraints and Their Effect on System Design

The legal requirements identified in Sections 4 and 5 impose specific constraints on technical design choices. Rather than limiting what is technically possible, these constraints establish a framework within which implementation decisions must operate. Each constraint derives from established evidentiary law and forensic standards, ensuring that any compliant system can withstand judicial scrutiny under both Daubert and Frye standards.

7.1.1 Authentication Requirements Under FRE 901

Federal Rule of Evidence 901 requires that evidence be authenticated through distinctive characteristics before admission at trial. For blockchain chain of custody systems, this requirement necessitates cryptographic mechanisms that uniquely identify each piece of evidence and link it to an immutable custody record. A legally compliant system must generate cryptographic hashes that serve as digital fingerprints for evidence items, enabling authentication without requiring the physical evidence to be present during every custody transfer or court proceeding.

The system employs SHA-256 hashing to satisfy this authentication requirement. When evidence enters the chain of custody, the system generates a SHA-256 hash from either the digital evidence file itself or, for physical evidence, from photographs and detailed measurements recorded at collection. This hash becomes the evidence item's unique identifier throughout its lifecycle. Each custody record stored on the blockchain references this hash, creating an immutable link between the blockchain entry and the actual evidence. If the evidence is altered—whether through tampering, degradation, or legitimate forensic analysis—rehashing will produce a different value, immediately alerting all parties to the change. This mechanism provides the "distinctive characteristics" that FRE 901(b)(4) requires for authentication while creating a tamper-evident audit trail that satisfies chain of custody documentation requirements.

Following the data structure approach presented in Bonomi et al., each blockchain record contains only metadata about the evidence—case identifiers, custody transfer information, timestamps, and the cryptographic hash—while the actual evidence remains in secure off-chain storage. This separation ensures that the blockchain record itself constitutes sufficient authentication under FRE 901 without requiring the blockchain to store sensitive or voluminous evidence data.

7.1.2 Expert Testimony Requirements Under Daubert and Frye

Expert testimony on blockchain technology for chain of custody purposes occupies a unique position: the field is sufficiently established to have proven cryptographic foundations, yet sufficiently novel in legal contexts to lack extensive case law. This tension requires careful selection of components that can satisfy both Daubert's multifactor reliability test and Frye's general acceptance standard. The system must employ only those algorithms and techniques that possess robust peer review, real-world validation, and formal standardization by recognized authorities.

SHA-256 satisfies these requirements through its extensive validation history and official standardization. Approved by the NIST under FIPS 180-4 [35], SHA-256 has been subjected to decades of cryptanalytic scrutiny and is deployed across billions of applications worldwide. An expert witness testifying about SHA-256 can cite this extensive body of validation without needing to defend the algorithm's fundamental soundness. Similarly, RSA digital signatures, standardized under NIST FIPS 186-4 [36], provide the authentication mechanism for custody transfers with comparable levels of peer review and real-world testing.

The choice of consensus mechanism presents a more nuanced challenge. While numerous consensus algorithms exist, Practical Byzantine Fault Tolerance offers particular advantages for satisfying evidentiary standards. Published by Castro and Liskov in 1999 [37], PBFT has been extensively studied in academic literature and possesses formal mathematical proofs of its fault tolerance properties. This mathematical foundation allows expert witnesses to provide concrete, testable claims about system reliability rather than relying on empirical observation alone. Furthermore, PBFT's prominence in the technical literature reviewed in Section 3 – where multiple independent research teams converged on PBFT as their consensus mechanism of choice – strengthens claims of "general acceptance" under Frye [25]. The repeated validation of PBFT across different implementations by different researchers provides evidence of consensus within the relevant scientific community.

PBFT's use of Proof of Authority [39] for validator selection offers additional legal advantages. Under PoA, designated authorities – in this context, court administrators, law enforcement IT departments, and forensic laboratories – would serve as the validator nodes. This approach eliminates the cryptographic complexity and economic incentive structures present in Proof of Work or Proof of Stake systems, replacing them with straightforward institutional accountability. A judge or jury can readily understand that trusted government agencies validate custody transfers without requiring extensive testimony about mining, staking, or cryptoeconomic game theory. This accessibility reduces the expert testimony burden while maintaining the Byzantine Fault Tolerance properties that blockchain consensus provides.

The convergence of these three components – SHA-256 for hashing, RSA for signatures, and PBFT for consensus – creates a system whose technical foundations can be defended under both Daubert and Frye with minimal evidentiary burden. Each component has been tested, peer-reviewed, standardized, and widely accepted. Expert witnesses can reference decades of validation rather than arguing for acceptance of novel approaches. This conservative technical posture trades potential performance optimizations for legal defensibility, embodying the thesis's central principle that adoption depends on satisfying evidentiary standards rather than achieving technical sophistication.

7.1.3 Destruction Orders under U.S.C. § 3509 and *Comprehensive Drug Testing*

The data architecture of any blockchain chain of custody system must accommodate legal requirements that directly conflict with blockchain's defining characteristic: immutability. Courts sometimes issue orders requiring evidence to be returned, destroyed, or sealed – actions that cannot be executed if evidence data resides permanently on an immutable ledger. This tension between blockchain's technical properties and legal necessity mandates a hybrid architecture that separates custody records from evidence storage.

The legally compliant architecture maintains a clear separation: the blockchain stores only metadata about evidence (cryptographic hashes, custody transfer records, timestamps, access logs), while actual evidence resides in conventional secure storage systems with access controls and destruction capabilities. This approach has been corroborated by existing work [17] [18]. When a court orders evidence destroyed, the physical or digital evidence can be removed from storage while the blockchain record of its custody history remains intact, and can be updated to reflect its destruction. Future audits can verify that custody protocols were observed even though the evidence itself no longer exists.

7.1.4 Inadvertent Disclosure Under FRE 502

This architectural separation also addresses inadvertent disclosure scenarios governed by Federal Rule of Evidence 502. When privileged or work-product materials are accidentally included in evidence production, FRE 502(b) allows parties to "claw back" those materials if the disclosure was inadvertent and the producing party took reasonable steps to prevent disclosure and rectify the error. Blockchain immutability would make such clawback impossible if the privileged materials were stored on-chain. By maintaining evidence in off-chain storage, the system allows privileged materials to be returned or destroyed per court order while the blockchain retains a record that the material existed, was disclosed inadvertently, and was subsequently returned under FRE 502 procedures. This preserves the audit trail without perpetuating the disclosure.

7.1.5 NIST Networking Requirements

Drawing from NIST IR 8387 [11], we can define the particular functions of the system. Alongside our previously defined legal constraints, a tangible system begins to emerge. The system must be able to document the original source of the evidence and the transfer details. These details should likely be placed in local storage as to preserve the security of the case. NIST approved hashes can be applied to the physically stored digital object as well and reflected in the blockchain metadata. NIST IR 8387 suggests that hashes be generated proximal to the initial collection of the evidence. Thus, the system should not produce its own SHA-256 hashes, but allow manual entry of already-produced hashes. Thus, the onus to assign a correct hash falls to the digital forensics investigator. Lastly, the blockchain should be permissioned and private, in correspondence with the NIST IR 8387's secure cloud networking requirements. In addition to resolving the consequences derived from destruction orders and Federal Evidence Rules, the NIST also mandates that evidence "be kept in a system that is not connected to the internet." That said, a permissioned blockchain effectively restricts access from public devices, providing protection against malicious actors.

7.3 Architecture

7.3.1 Architecture Overview

The reference architecture consists of three primary components: (1) The Evidence Registry smart contract manages the storage of evidence metadata records. The contract also supports the transfer of ownership between parties; (2) Access control mechanisms will provide role-based permissions to parties ensuring that only authorized parties can submit or transfer evidence items; (3) An off-chain database will contain evidence objects consisting of the physical data of the on-chain blockchain reference, as well as relevant metadata like file hashes and ownership. The off-chain SHA-256 file hash will be used as reference to the on-chain record, which will be able to detect any changes to data over the lifecycle of the evidence.

7.3.2 Deployment Architecture

Similar to the structure presented by Bonomi, et al. [18], our system will designate different jurisdictions as custodians of the blockchain's nodes. The nodes will comprise a permissioned blockchain, utilizing Practical Byzantine Fault Tolerance [36] as its consensus mechanism. PBFT will require $3f + 1$ nodes, where f is the number of faulty nodes. A sufficiently large system, such as the one proposed here, can handle this requirement. PBFT comes equipped with significant academic rigor and predictable failure rates, satisfying previously defined legal requirements.

Real-world deployment would require a bespoke blockchain implementation, which is beyond the scope of this thesis. However, any implementation must be permissioned and support smart contract capabilities. A permissioned Ethereum fork would suffice [37], however more research must be done to understand the complete technical implications.

Off-chain storage, one of the most important aspects of a legally-compliant blockchain framework, minimizes the blockchain's storage burden. This database will contain the actual digital evidence associated with the blockchain records. Any incongruence between on-chain file hash data and database file hash data would be efficiently tracked and recorded.

More bespoke design details will be left for future work, as many of the technical implementations require significant monetary investment and testing. This architecture is only to provide a high-level overview of the components of a legally defensible system.

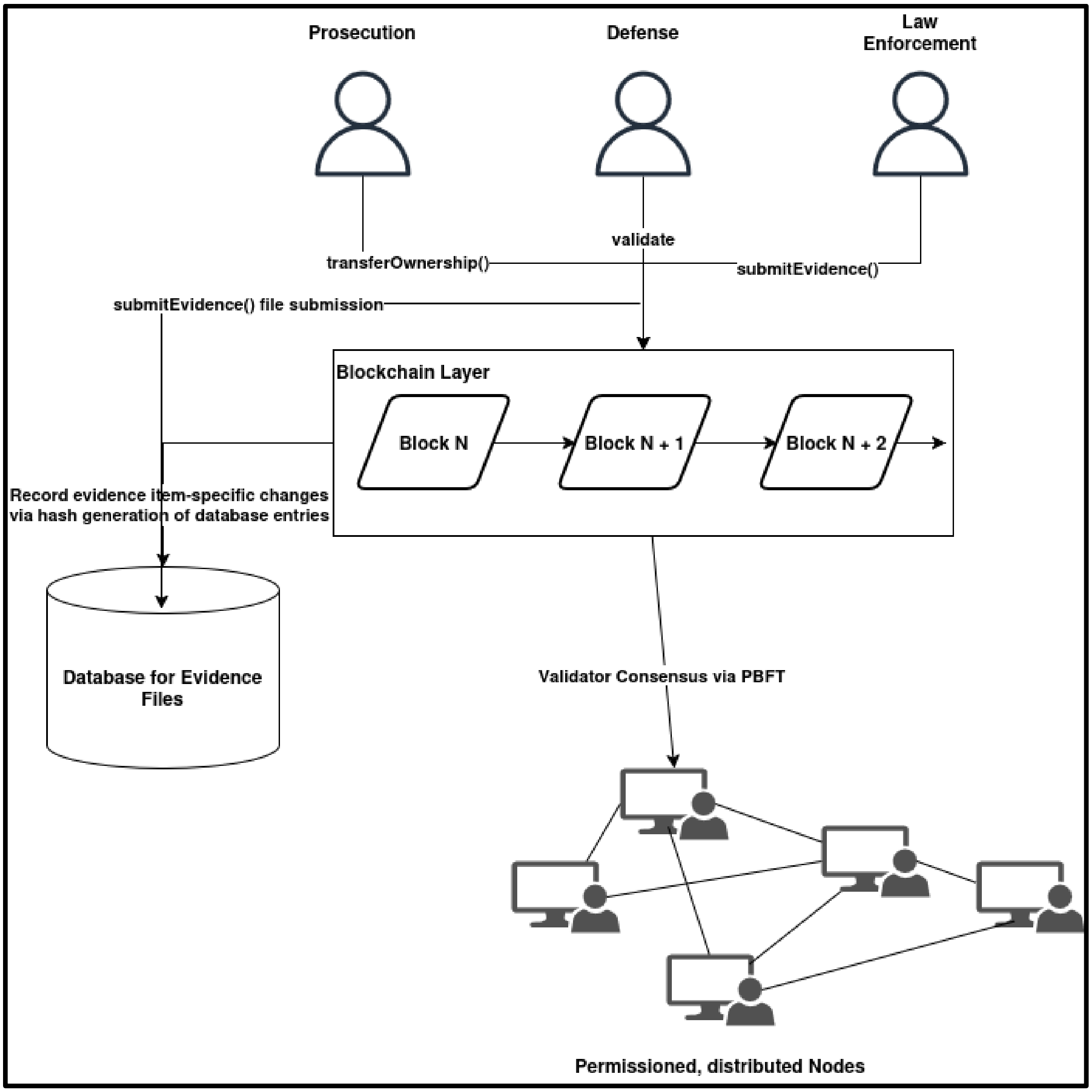

Figure 7.1: High-Level Reference Architecture Overview

8 Future Work

Future research should focus on prototype validation, interoperability testing, and statutory alignment. A working implementation – even a limited one – would allow empirical evaluation of performance metrics (throughput, latency, node fault tolerance) against the system's evidentiary obligations. Pilot programs within small jurisdictions or specialized agencies (for instance, government-led digital forensics divisions) could produce the first case law references to blockchain-based custody records. These statistics could then be used as justification for the adoption of more innovative modules, such as more effective consensus mechanisms and modular blockchains.

Interoperability between blockchain and existing law enforcement databases remains a critical challenge. Future iterations should explore standardized APIs or middleware capable of bridging blockchain transactions with systems like the FBI's Digital Evidence Management System or state-level equivalents.

High-level architectural design – integrating blockchain into the existing decentralized criminal court structure – is of great importance when designing a large-scale system. Similar to Bonomi, et al., future research should look at how different federal circuits, state courts, municipal courts, and county courts divide custodianship and access. Perhaps, each jurisdiction should maintain a blockchain independent of one another. Contrarily, each blockchain could belong to an interoperable blockchain, where individual blockchains maintain their own records, but nodes operate on the same network, providing additional compute and decentralization.

Additional scholarship is required to align blockchain evidence handling with statutory requirements. While blockchain may be able to adapt to many different evidentiary requirements, altering the law to accommodate blockchain's increased security may be a better way of addressing its shortcomings.

Finally, a comprehensive cost-benefit analysis in comparison to traditional systems must be performed. Though technical optimizations are possible, it must be known whether or not blockchain's unique security benefits outweigh the cost of infrastructure required to implement such a system.

9 Limitations

This thesis establishes a legal framework for blockchain chain of custody systems, but several limitations constrain the scope and applicability of this work.

The reference architecture presented in Section 7 remains theoretical. Without a working prototype or pilot implementation, critical questions about performance, scalability, and real-world usability remain unanswered. The system's actual throughput under high-volume evidence submission, its behavior during network failures or validator node compromises, and the practical challenges of multi-jurisdictional coordination cannot be fully assessed without deployment testing. While the technical components (SHA-256, RSA, PBFT) have established reliability metrics in other contexts, their integration into a chain of custody system requires empirical validation that this thesis does not provide.

This work does not evaluate implementation costs or compare them against traditional chain of custody systems. Blockchain deployment requires significant infrastructure investment—server hardware for validator nodes, network configuration, software development, staff training, and ongoing maintenance. Courts and law enforcement agencies operate under strict budgetary constraints. Without demonstrating that blockchain systems offer cost savings, efficiency gains, or risk reduction sufficient to justify these expenses, practical adoption remains uncertain regardless of legal compliance. Future work must quantify both implementation costs and potential benefits (reduced evidence handling errors, decreased Brady violation litigation, improved audit efficiency, etc.) to make an economic case for adoption.

The legal analysis primarily addresses Federal Rules of Evidence and federal court standards. However, the United States criminal justice system is highly decentralized. State courts, which handle the vast majority of criminal cases, may operate under different evidentiary rules. As noted in Section 4.3, California and New York apply the Frye standard rather than Daubert, potentially creating different admissibility thresholds. Additionally, individual jurisdictions may have specific chain of custody requirements, evidence handling protocols, or administrative rules that impose constraints beyond those analyzed here. That said, many state courts operate under statutes very similar to the Federal Evidence Rules, making translation more simplistic than not.

10 Conclusion

Analysis of existing case law, Federal Evidence Rules, judicial standards, NIST guidelines, and legal reviews reveals that existing blockchain chain of custody research likely suffers from regulatory shortcomings that prevent practical adoption. That said, when placed under scrutiny, some literature [18] provides a reasonable foundation from which a United States-based blockchain chain of custody architecture can emerge.

This thesis has demonstrated that existing literature largely fails in establishing a legal baseline from which admissibility can be derived. The Technical Literature Review presented in Section 3 reveals a lack of deference to any governing authority, even when certain aspects may be legally compliant.

Sections 4 and 5 elucidated these shortcomings through a legal review, concluding that blockchain architecture, under current evidentiary laws, must maintain separation between physical evidence data and evidentiary records, and employ widely-tested technical components. Importantly, under the Daubert and Frye standards, technical simplicity contributes more greatly to the eventual adoption than rigorous system sophistication.

Section 6 provided a retroactive analysis of the technical papers presented in section 3, underscoring the legal veracity of Bonomi, et al [18]. The majority of papers introduced unnecessary technical sophistication that drove their architecture further from eventual adoption under Daubert and Frye. In comparison, Bonomi et al. relied upon widely-accepted technical components such as Ethereum and Practical Byzantine Fault Tolerance, while introducing a distributed blockchain system whose infrastructure could be readily translated to the United States' decentralized court structure.

Drawing from many of the components presented in Bonomi, et al. [18], section 7 introduced a reference architecture alongside legal justification for each of the tools employed. The section provided a high-level overview of a potentially viable system, without extensive technical details. NIST-approved hashing algorithms like SHA-256 and RSA encryption were cited as effective components in a larger architecture. Off-chain evidence storage and the PBFT consensus mechanism rounded out this reference architecture. For the blockchain itself, a permissioned Ethereum fork was suggested as a viable solution, however this thesis defers to future research to provide a more substantive solution.

The path forward requires collaboration between technologists, legal scholars, and judicial administrators. Pilot programs should begin at the local or state level, allowing courts to develop case law precedent that clarifies blockchain's evidentiary status. As these systems prove themselves in limited deployments, the legal community's comfort with blockchain technology will grow, potentially enabling the sophisticated optimizations that current research proposes.

This work demonstrates that the question is not whether blockchain can improve chain of custody, but rather how to design systems that courts will accept. By prioritizing legal compliance over technical innovation, blockchain chain of custody can move from theoretical possibility to practical reality, ultimately serving its intended purpose: protecting the integrity of evidence and, by extension, the integrity of justice itself.

Bibliography

[1]M. Ryan, "Daubert Standard," *Legal Information Institute*, 2018. https://www.law.cornell.edu/wex/daubert_standard

[2] Cornell Law School, "Rule 901. Authenticating or Identifying Evidence," *LII / Legal Information Institute*, 2011. https://www.law.cornell.edu/rules/fre/rule_901

[3] A. Badiye, N. Kapoor, and R. Menezes, "Chain of Custody (Chain of Evidence)," *PubMed*, Feb. 13, 2023. https://www.ncbi.nlm.nih.gov/books/NBK551677/

[4] "Robinson v. Commonwealth," *Justia Law*, 1971. https://law.justia.com/cases/virginia/supreme-court/1971/7481-1.html (accessed Oct. 28, 2025).

[5] Cornell Law School, "Brady Rule," *LII / Legal Information Institute*, Jan. 2023. https://www.law.cornell.edu/wex/brady_rule

[6] T. M. Joslyn and S.-T. Regon, "NACDL - Faces of Brady: The Human Cost of Brady Violations," *NACDL - National Association of Criminal Defense Lawyers*, 2013. https://www.nacdl.org/Article/May2013-FacesofBradyTheHumanCostofBrad

[7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *National Institute of Standards and Technology*, vol. 1, no. 1, Oct. 2018, doi: https://doi.org/10.6028/nist.ir.8202.

[8] Ethereum Community, "Introduction to smart contracts | ethereum.org," *ethereum.org*, Feb. 12, 2025. https://ethereum.org/developers/docs/smart-contracts/

[9] United States Courts, "Court Role and Structure," *United States Courts*, 2025. https://www.uscourts.gov/about-federal-courts/court-role-and-structure

[10] J. Wilets and A. Imoukhuede, "A Critique Of The Uniquely Adversarial Nature Of The U.S. Legal, Economic And Political System And Its Implications For Reinforcing Existing Power Hierarchies," 1987. Available: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1214&context=jlasc

[11] B. Guttman, D. White, and T. Walraven, "Digital Evidence Preservation," *Digital Evidence Preservation*, Sep. 2022, doi: https://doi.org/10.6028/nist.ir.8387.

[12] United States v. Comprehensive Drug Testing Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc). Available: https://cdn.ca9.uscourts.gov/datastore/opinions/2010/09/13/05-10067.pdf

[13] Cornell Law School, "Rule 502. Attorney-Client Privilege and Work Product; Limitations on Waiver," *LII / Legal Information Institute*. https://www.law.cornell.edu/rules/fre/rule_502

[14] M. Boughdiri, T. Abdellatif, and C. Ghedira Guegan, "A Systematic Literature Review on Blockchain Storage Scalability," *IEEE Access*, vol. 13, pp. 102194–102219, 2025, doi: https://doi.org/10.1109/access.2025.3578451

[15] X. Wang, Ying Cheng Wu, and Z. Ma, "Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes," *Frontiers in blockchain*, vol. 7, Apr. 2024, doi: https://doi.org/10.3389/fbloc.2024.1306058.

[16] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," *Digital Investigation*, vol. 28, pp. 44–55, Mar. 2019, doi: https://doi.org/10.1016/j.diin.2019.01.002.

[17] K. M. M. Salih and N. B. Ibrahim, "CustodyChainGuardian: Blockchain of Custody Digital Evidence Preservation System," pp. 168–175, Dec. 2023, doi: https://doi.org/10.1109/agers61027.2023.10490757.

[18] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics," *arXiv:1807.10359 [cs]*, Jul. 2018, doi: https://doi.org/10.4230/OASIcs.Tokenomics.2019.12.

[19] United States Sentencing Commission, "Annual Report 2024," *United States Sentencing Commission*, Mar. 10, 2025. https://www.ussc.gov/about/annual-report-2024

[20] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, Jul. 2019, doi: https://doi.org/10.1016/j.ins.2019.04.011.

[21] L. Ahmad, S. Khanji, F. Iqbal, and F. Kamoun, "Blockchain-based chain of custody," *Proceedings of the 15th International Conference on Availability, Reliability and Security*, Aug. 2020, doi: https://doi.org/10.1145/3407023.3409199.

[22] Cornell Law School, "Rule 902. Evidence That Is Self-Authenticating," *LII / Legal Information Institute*. https://www.law.cornell.edu/rules/fre/rule_902

[23] Cornell Law School, "Rule 1002. Requirement of the Original," *LII / Legal Information Institute*. https://www.law.cornell.edu/rules/fre/rule_1002

[24] Justia, "Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)," *Justia Law*, 1993. https://supreme.justia.com/cases/federal/us/509/579/

[25] Cornell Law School, "Frye Standard," *LII / Legal Information Institute*, 2022. https://www.law.cornell.edu/wex/frye_standard

[26] "State-by-State Compendium Standards of Evidence." Available: https://ncji.org/wp-content/uploads/2024/01/Evidence-Standards-by-State-7.12.23.pdf

[27] Cornell Law School, "18 U.S. Code § 3509 - Child victims' and child witnesses' rights," *LII / Legal Information Institute*. https://www.law.cornell.edu/uscode/text/18/3509

[28] Cornell Law School, "Rule 502. Attorney-Client Privilege and Work Product; Limitations on Waiver," *LII / Legal Information Institute*. https://www.law.cornell.edu/rules/fre/rule_502

[29] Cornell Law School, "Rule 801. Definitions That Apply to This Article; Exclusions from Hearsay," *LII / Legal Information Institute*. https://www.law.cornell.edu/rules/fre/rule_801

[30] United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015). Available: https://law.justia.com/cases/federal/appellate-courts/ca9/13-10530/13-10530-2015-06-18.html

[31] Cornell Law School, "Rule 803. Exceptions to the Rule Against Hearsay," *LII / Legal Information Institute*, 2022. https://www.law.cornell.edu/rules/fre/rule_803

[32] American Academy of Forensic Sciences, "What Is Forensic Science?," *AAFS*, 2023. https://www.aafs.org/careers-forensic-science/what-forensic-science

[33] E. Knight, "Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility under the Federal Rules," *Scholarship @ Hofstra Law*, 2019. https://scholarlycommons.law.hofstra.edu/hlr/vol48/iss2/8/

[34] "The DAO: What Was the DAO and How Was it Hacked?," *Gemini*, Feb. 27, 2025. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

[35] N. I. of S. and Technology, "Secure Hash Standard (SHS)," *csrc.nist.gov*, Aug. 04, 2015. https://csrc.nist.gov/pubs/fips/180-4/upd1/final

[36] N. I. of S. and Technology, "Digital Signature Standard (DSS)," *csrc.nist.gov*, Jul. 19, 2013. https://csrc.nist.gov/pubs/fips/186-4/final

[37] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: https://doi.org/10.1145/571637.571640.

[38] J. Polge, J. Robert, and Y. Le Traon, “Permissioned blockchain frameworks in the industry: A comparison,” *ICT Express*, vol. 7, no. 2, Sep. 2020, doi: https://doi.org/10.1016/j.icte.2020.09.002.

[39] “A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique,” *ieeexplore.ieee.org*. https://ieeexplore.ieee.org/document/9860157