WitnessApp: Infrastructure for Accessible Justice

Abstract

Millions experience injustice they cannot prove. WitnessApp explores how cryptographic timestamps and privacy-preserving coordination might transform smartphones into tools for justice. By creating tamper-proof documentation, enabling anonymous pattern discovery, and facilitating collective action, we envision making justice infrastructure as accessible as sending a text. While blockchain evidence shows promise in early court decisions globally [1,2,3], significant legal and technical work remains. This paper outlines a vision for temporal sovereignty—owning your timeline through cryptographic proof—and invites legal professionals, technologists, and advocates to help build this future.

1. The Justice Gap

1.1 The Documentation Divide

Justice requires evidence, but evidence requires resources. Those who can afford lawyers receive coaching on documentation. Those who cannot—the vast majority—face injustice with empty hands [10]. A manager's discriminatory comment vanishes into air. A landlord's promise becomes selective memory. A pattern of abuse remains invisible because its victims stay isolated.

We observe a temporal dimension to this gap [11]. Power seems to exploit time through delay, erosion of memory, and isolation. By the time victims find others with similar experiences, evidence often disappears. Could technology help level this playing field?

1.2 The Isolation Trap

Abusive systems appear to thrive on engineered isolation. Each victim believes they're alone, too afraid to speak first. HR departments that handle complaints "internally." Academic committees that resolve things "quietly." Medical systems where patient concerns vanish into unread charts [12].

What if breaking isolation didn't require exposure first? What if people could discover shared experiences while maintaining privacy until ready to act? This inverts the traditional model where courage must come before connection [16].

2. A Vision for Temporal Sovereignty

2.1 The Promise of Cryptographic Time

WitnessApp explores temporal sovereignty: the concept that individuals might own their timeline through cryptographic proof. Using Bitcoin's blockchain as a timestamping service [6]—an approach showing early promise in courts—every recorded experience could receive mathematical proof of when it was documented [9].

While legal frameworks are still evolving, early precedents suggest potential. China's Internet Courts have experimented with blockchain evidence since 2018 [1,2]. The U.S. Bitcoin Fog case demonstrated blockchain analytics can meet evidentiary standards [3]. Yet significant questions remain about admissibility, authentication, and implementation across jurisdictions [13].

2.2 Privacy-Preserving Connection

Our core hypothesis: anonymous pattern matching could break isolation safely. Users might discover others with similar experiences without revealing themselves until mutual consent is established [8]. Think dating app mechanics applied to justice—but with cryptographic privacy protection.

Imagine if a woman facing workplace harassment could learn others have documented similar experiences, without any individual exposing themselves first. The technical foundations exist [7,20], but the legal and social frameworks need development.

3. Proposed Capabilities

3.1 Capture: Building Toward Admissibility

Documentation could be as simple as:

- **Voice**: Record incidents with encrypted storage [19]
- **Photo**: Capture evidence with cryptographic timestamps
- **Text**: Quick notes with blockchain proof of creation time

The challenge: working with legal professionals to understand what makes digital evidence admissible across jurisdictions [13,15]. How can we format timestamps to meet authentication requirements? What metadata must be preserved? These questions require deep collaboration with legal experts.

3.2 Connect: Exploring Safe Discovery

We envision pattern matching that enables:

- **Anonymous Search**: "Has anyone else experienced similar treatment?"
- **Threshold Revelation**: Identity revealed only after multiple matches [16]
- **Progressive Disclosure**: Share details in stages as trust builds

Zero-knowledge proofs offer technical solutions [8,20], but the legal implications need exploration. How do courts view evidence gathered through anonymous coordination? What consent frameworks are required [14]?

3.3 Coordinate: From Individual to Collective

When isolation breaks, we hypothesize coordination emerges:

- **Pattern Documentation**: Show systematic behavior [17]
- **Timeline Aggregation**: Build collective narratives
- **Evidence Preparation**: Format for legal proceedings

The opportunity: transform individual documentation into collective accountability. The challenge: ensuring group coordination maintains individual agency and consent [21].

4. Early Evidence and Open Questions

4.1 Emerging Legal Precedents

Courts worldwide are beginning to grapple with blockchain evidence:

- **China**: Internet Courts accepting blockchain timestamps [1,2] (needs broader adoption)
- **USA**: Bitcoin Fog case suggests openness to blockchain analytics [3] (narrow ruling)
- **EU/UK**: Existing digital evidence frameworks might apply [5,14] (untested for timestamps)
- **Singapore**: Recognition of smart contracts and crypto as property [4]

We need legal scholars and practitioners to help navigate:

- Authentication requirements across jurisdictions [13]
- Chain of custody for digital evidence [15]
- Privacy law compliance for pattern matching [14]
- Ethical frameworks for anonymous coordination

4.2 Technical Possibilities and Challenges

Promising approaches need validation:

- **Client-side encryption**: Protecting evidence at rest [19]
- **Distributed architecture**: Avoiding central points of failure
- **Offline functionality**: Ensuring universal access
- **Panic features**: Safety in dangerous situations [22]

Open questions requiring research:

- Long-term storage and availability [18]
- Cross-device synchronization security
- Biometric authentication reliability
- Cultural adaptation for global use [22,23]

5. Theory of Change (Hypothesis)

5.1 Potential Cascade Effects

We hypothesize change might flow through stages:

1. **Individual**: People document experiences safely
2. **Discovery**: Anonymous matching reveals patterns
3. **Collective**: Groups coordinate evidence
4. **Institutional**: Organizations face pattern documentation
5. **Systemic**: Legal and policy frameworks evolve

This remains theoretical. Pilot programs could test whether documentation leads to connection, connection to coordination, and coordination to change [11,12].

5.2 Questions for Exploration

Critical unknowns need investigation:

- Will people trust anonymous matching?
- Can collective evidence overcome individual testimony's power?
- How do institutions respond to pattern documentation?
- What unintended consequences might emerge?

6. Sustainability and Governance

6.1 Exploring Economic Models

We believe justice infrastructure shouldn't extract rent from vulnerable users [10]. Potential approaches:

- Foundation funding for public good technology
- Legal aid organization partnerships
- Government grants for access to justice [11]
- Sliding scale for institutional users

The challenge: sustainable funding without compromising mission.

6.2 Open Development Philosophy

We propose open source development because:

- Transparency builds trust
- Community review improves security
- No vendor lock-in protects users
- Collective ownership ensures longevity [23]

Questions remain about governance, contribution models, and sustainability.

7. Invitation to Build Together

To Legal Professionals

Help us navigate the path from promising technology to admissible evidence. What requirements must we meet [13,15]? How can we format documentation for courts? What ethical frameworks should guide anonymous coordination? Your expertise can shape whether this vision becomes reality.

To Foundations and Funders

This is an exploration of justice as infrastructure. We need patient capital to research, pilot, and iterate. Fund not just technology but the legal frameworks, community partnerships, and careful deployment that systemic change requires [10,11].

To Technologists

Complex challenges await: privacy-preserving coordination [7,8,20], secure evidence storage, accessible interfaces. Help us build technology that disappears into the background while empowering those who need it most.

To Communities and Advocates

Your experiences and needs must guide development [22,23]. What features would help? What concerns need addressing? How can we ensure the technology serves justice, not surveillance?

Conclusion: An Invitation to Explore

WitnessApp represents a question: Can we make justice infrastructure as accessible as communication infrastructure? Can temporal sovereignty—owning your timeline through cryptographic proof—help level playing fields tilted by power?

We don't have all the answers. Legal frameworks need development. Technical challenges remain. Social acceptance requires building. But the potential—transforming phones into tools for justice, isolation into connection, individual vulnerability into collective strength—demands exploration.

This isn't a finished solution but an invitation. To lawyers: help us navigate admissibility. To funders: enable careful experimentation. To technologists: solve the hard problems. To communities: guide our development.

Together, we might build a future where truth doesn't require wealth, where justice doesn't require permission, where time belongs to those who live it.

The question isn't whether it's fully solved—it's whether it's worth solving together.

Join us in exploring how time might become a tool for justice.

References

Legal Precedents and Frameworks

[1] Hangzhou Internet Court. "First Case Recognizing Blockchain Evidence" (June 2018). Huatai Yimei Ltd. v. Daotong Ltd. [Chinese language source]

[2] Supreme People's Court of China. "Provisions on Several Issues Concerning the Trial of Cases by Internet Courts" (September 2018). Articles 11-12 on blockchain evidence.

[3] United States v. Sterlingov, No. 21-cr-399 (D.D.C. 2024). "Bitcoin Fog Case: Daubert ruling on blockchain analytics admissibility"

[4] B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03. Singapore International Commercial Court recognition of smart contracts and cryptocurrency as property.

[5] UK Jurisdiction Taskforce. "Legal Statement on Cryptoassets and Smart Contracts" (November 2019). The LawTech Delivery Panel.

Technical Foundations

[6] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008). Original Bitcoin whitepaper establishing blockchain timestamping.

[7] Gennaro, R., et al. "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems" (1999). Foundations for distributed cryptographic protocols.

[8] Ben-Sasson, E., et al. "Zerocash: Decentralized Anonymous Payments from Bitcoin" (2014). Zero-knowledge proof systems for privacy.

[9] OpenTimestamps.org. "A timestamping proof standard" (2016). Open protocol for blockchain timestamping.

Access to Justice Research

[10] Legal Services Corporation. "The Justice Gap: Measuring the Unmet Civil Legal Needs of Low-income Americans" (2022).

[11] OECD. "Equal Access to Justice for Inclusive Growth" (2019). Framework for understanding justice accessibility.

[12] The Hague Institute for Innovation of Law. "Justice Needs and Satisfaction Study" (2021). Global justice gap analysis.

Digital Evidence Standards

[13] Scientific Working Group on Digital Evidence (SWGDE). "Digital Evidence: Standards and Principles" Version 2.0 (2019). Available at: https://www.swgde.org/

[14] European Union Agency for Cybersecurity. "eIDAS Regulation on electronic identification and trust services" (2014).

[15] ISO/IEC 27037:2012. "Guidelines for identification, collection, acquisition and preservation of digital evidence"

Related Initiatives

[16] Callisto. "Creating Options to Report Sexual Assault" (2015-present). Platform for matching sexual assault reports. https://www.projectcallisto.org

[17] Amnesty International. "Citizen Evidence Lab: Using open source methods for human rights research" (2020). Available at: https://citizenevidence.org/

[18] Syrian Archive. "Preserving documentation of human rights violations" (2014-present). Digital evidence preservation. https://syrianarchive.org

Technical Resources

[19] Signal Protocol. "End-to-end encryption specification" (2016). Foundation for secure messaging.

[20] Bulletproofs. "Short Proofs for Confidential Transactions and More" (2018). Efficient zero-knowledge proofs.

[21] W3C. "Decentralized Identifiers (DIDs) v1.0" (2022). Standards for self-sovereign identity.

Trauma-Informed Design

[22] SAMHSA. "Trauma-Informed Care in Behavioral Health Services" (2014). Treatment Improvement Protocol (TIP) Series 57.

[23] Design Justice Network. "Design Justice Principles" (2018). Community-led design practices.

Contact and Collaboration

Research Collaboration: research@witnessapp.org
Legal Framework Development: legal@witnessapp.org
Technical Contributors: dev@witnessapp.org
Pilot Partnerships: pilots@witnessapp.org
Foundation Relations: impact@witnessapp.org

Acknowledgments

This vision builds on decades of work by legal aid organizations, technologists, and advocates fighting for accessible justice. Special recognition to the survivors and witnesses whose courage in documenting truth, despite systems designed to silence them, inspires this work.

Document Version 1.0 - July, 2025
This white paper is licensed under Creative Commons CC BY-SA 4.0
Cite as: WitnessApp Collective. "WitnessApp: Infrastructure for Accessible Justice" (2025)