Zera Labs

The Texas Privacy-First Digital Finance Act

> **This presents an extraordinary opportunity for the Lone Star state to assert its leadership**, not merely as a participant in the digital asset economy, but as its primary architect and constitutional guardian.

Hayden "Dax" Porter
dax@zeralabs.org

Executive Summary

Texas stands at a pivotal moment in American History. With privacy and security under threat across the grand republic one of the most dear things we can rely on is our wallets. Federal regulators on both sides of the isle have escalated their attacks on privacy-preserving technologies, which has recently culminated in the unprecedented sanctioning of the Tornado Cash protocol. As a result a regulatory vacuum has emerged.

This presents an extraordinary opportunity for the Lone Star state to assert its leadership, not merely as a participant in the digital asset economy, but as its primary architect and constitutional guardian.

The recent court victories against federal overreach in the Tornado Cash case, combined with Texas's own groundbreaking establishment of the Strategic Bitcoin Reserve, demonstrate both the vulnerability of centralized, enforcement-first regulatory approaches and the power of forward-thinking state-level policy. Building on this momentum, the Texas Privacy-First Digital Finance Act represents the next logical evolution: a comprehensive legislative framework that protects individual liberty, fosters permission-less innovation, and ensures what happened to Tornado Cash is constitutionally impossible in Texas.

The Solution:
The Texas Privacy-First Digital Finance Act

This policy book outlines a complete legislative framework **to establish Texas as the world's premier jurisdiction for privacy-preserving financial technology**. The Act provides clear statutory protections for mathematically sound privacy protocols, creating a regulatory environment that attracts investment and talent while maintaining robust consumer protection and compliance mechanisms.

Drawing upon the groundbreaking research conducted by engineers who have co-authored this proposal directly from Zera Labs, the Act establishes objective, verifiable standards grounded in cryptographic science.

Hayden “Dax” Porter
dax@zeralabs.org

Core Innovation:
Mathematical Soundness as a Legal Standard

The Act's most revolutionary feature is its recognition of mathematical soundness as a legal standard for protecting privacy protocols. This approach moves beyond subjective regulatory interpretations and instead creates a safe harbor for technologies that can formally prove their security and integrity.

Based on industry standard definitions demonstrating reasonable security and proven mathematical hardness, the legislation establishes that **protocols meeting these rigorous mathematical criteria deserve explicit legal protections.**

Technical Foundation:
Proven Privacy Infrastructure

The legislative framework of this Act is grounded in cryptographic principles that are both **mathematically proven and commercially adopted**, while also anticipating the security needs of the future.

The policies herein are designed to support and protect the entire lifecycle of cryptographic innovation, from established standards that **secures today's digital economy to the next-generation systems that will protect it from future threats.**

Hayden "Dax" Porter
dax@zeralabs.org

I. Core Cryptographic Primitives

These are the fundamental, peer-reviewed building blocks that enable secure and private digital transactions.

Zero-Knowledge Proofs (ZKPs):

A ZKP is a cryptographic protocol where one party (the prover) can prove to another party (the verifier) that a given statement is true, **without revealing any information beyond the statement's validity.** This is achieved by satisfying three core properties:

1. **Completeness:** If the statement is true, an honest prover can always convince an honest verifier.
2. **Soundness:** A dishonest prover cannot convince an honest verifier that a false statement is true, except with a negligible probability.
3. **Zero-Knowledge:** The verifier learns nothing except for the fact that the statement is true. All other information remains private.

Supporting Cryptographic Algorithms:

In addition to ZKPs themselves, the protocol relies on well-established cryptographic primitives that provide the mathematical backbone for secure commitments and encrypted balances:

Elliptic Curve Cryptography (ECC): A highly efficient and powerful approach to public-key cryptography that is based on the algebraic structure of elliptic curves over finite fields. ECC allows for smaller, faster, and more secure cryptographic keys compared to older methods like RSA, making it the standard for securing everything from web traffic (TLS/SSL) to modern digital signatures in financial protocols.

ElGamal Encryption: A public-key cryptosystem based on the mathematical difficulty of the Diffie-Hellman key exchange and the discrete logarithm problem. It is a well-established, asymmetric algorithm where encryption uses a public key and decryption requires a private key. Critically, ElGamal is probabilistic, meaning a single plaintext can result in many different ciphertexts, adding a layer of security.

ElGamal-Twist: As detailed in peer reviewed research, this is an advanced variant of ElGamal. It leverages specific properties of elliptic curves to add homomorphic capabilities, allowing computations (like adding balances) to be performed on encrypted data without ever decrypting it. This variant is essential for creating systems that are both private and auditable.

Hayden "Dax" Porter
dax@zeralabs.org

II. Privacy-Enhancing Network Architectures

Individual cryptographic methods are often deployed within larger network frameworks that are inherently designed to protect privacy.

In addition to ZKPs themselves, the protocols we seek to protect, relies on well-established cryptographic primitives that provide the mathematical backbone for secure commitments and encrypted balances:

Peer-to-Peer (P2P) Networks: These are decentralized networks where participants **(peers)** interact directly with each other to share resources and data without the need for a central coordinating server. This architecture enhances privacy by design, as there is no central point for data collection, surveillance, or failure. Commercial entities like **ThreeFold** are developing P2P cloud networks with a focus on user data control and privacy.

Virtual Private Networks (VPNs): A VPN creates a secure, encrypted "tunnel" for data transmission over a public network like the internet. By routing a user's traffic through a remote server, a VPN masks the user's IP address and encrypts their data, preventing third parties from monitoring their online activity. Major commercial providers with a stated focus on privacy include **Private Internet Access (PIA)** and **Hotspot Shield**.

Non-Custodial Systems (Self-Custody): A non-custodial system is one in which the user maintains sole and exclusive control of their private cryptographic keys. This is in direct contrast to custodial models, where a third-party (such as a bank or centralized exchange) holds the keys on behalf of the user. The principle of self-custody is fundamental to true digital asset ownership and privacy. It removes central points of failure and control, making it impossible for a third party to freeze, seize, or censor a user's assets. This model is exemplified by:

- **Hardware Wallets:** Devices from companies like Ledger and Trezor that store a user's private keys in a secure, offline environment.
- **Software Wallets:** Applications like MetaMask and Phantom that give the user direct control over their keys on their own computer or mobile device.

The end goal is to uphold the principle of separating the tool from the user. This is a foundational legal doctrine in American law. Just as manufacturers of lawful products are not held liable for their criminal misuse by independent third parties, developers who create and publish software or hardware should not be held responsible for the actions of individuals who use that technology.

To hold the innovator accountable for the user's actions would be a departure from centuries of legal precedent and would chill innovation and the development of secure, privacy-preserving tools for all Texans. **Responsibility must lie with the actor, not the inventor.**

Hayden "Dax" Porter
dax@zeralabs.org

III. Forward-Looking Security: Post-Quantum Cryptography (PQC)

To ensure long-term security, this Act also provides a framework for the development of encryption systems resistant to attacks from future quantum computers.

Lattice-Based Cryptography: A leading family of PQC that bases its security on the extreme difficulty of solving mathematical problems on high-dimensional geometric structures called lattices. These problems are believed to be hard for both classical and quantum computers, making lattice-based systems a robust foundation for future security. The U.S. National Institute of Standards and Technology (NIST) has selected lattice-based algorithms like CRYSTALS-Kyber for standardization.

Key Commercial and Research Entities: The race to develop and deploy PQC is being led by a diverse group of academic institutions and commercial firms, including:

- **Technology and Research Giants: IBM** and **Microsoft** are pioneering research and developing open-source libraries for lattice-based cryptography.
- **Hardware and Semiconductor Leaders: Infineon Technologies** is integrating PQC into hardware security modules.
- **Specialized PQC Firms:** Companies like **PQShield, Post-Quantum, Quantum Xchange**, and **MagiQ Technologies** are creating targeted PQC solutions, from quantum key distribution (QKD) to software libraries for IoT and financial services.

Hayden “Dax” Porter
dax@zeralabs.org

Economic Impact:
A New Frontier for Texas Prosperity

By establishing unparalleled regulatory clarity, the Texas Privacy-First Digital Finance Act will unleash a new wave of economic growth across the state. This legislation is projected to act as a powerful magnet for investment and talent, catalyzing a robust, self-sustaining innovation economy. Conservative projections indicate that within the fi rst fi ve years of its enactment, the Act will drive more than $2.4B in new private investment into Texas, funding the development of next-generation financial technologies.

This influx of capital will translate directly into high-quality jobs for Texans. We project the creation of over 15,000 direct, high-skilled positions in future-proof fi elds such as cryptography, blockchain engineering, and regulatory compliance. Furthermore, this boom will support an additional 35,000 indirect jobs in legal, financial, and technical services. The economic activity generated will substantially increase the state's revenue base, contributing an **estimated $180M in new state tax revenue and over $420M in local tax revenue** from property and sales taxes, directly benefiting Texas communities without burdening existing taxpayers.

Beyond direct financial metrics, the Act will serve as the foundation for a world-class privacy technology ecosystem. **We envision the establishment of an Austin Privacy Tech Hub, attracting over 150 companies and making Central Texas the global epicenter of this critical industry**. This will be supported by new academic and research partnerships with premier institutions like the University of Texas, Rice University, and Texas A&M, creating a powerful talent pipeline and ensuring that the foundational research for the future of finance happens here in Texas.

This innovation will spread across the state, creating new industry clusters that integrate privacy technology with traditional finance in Dallas, the energy sector in Houston, and the cybersecurity corridor in San Antonio, **securing Texas's role as a leader in the global digital economy for decades to come.**

Hayden “Dax” Porter
dax@zeralabs.org

A Framework for Freedom:
The Seven Pillars of the Act [1/2]

The Texas Privacy-First Digital Finance Act establishes a comprehensive and robust legal framework built on seven interconnected pillars. Each pillar is designed to protect individual rights, foster innovation, and ensure that Texas remains at the forefront of the digital economy while upholding the rule of law.

1. Explicit Statutory Protection for Privacy Protocols:

The Act removes legal ambiguity by formally codifying the legality of core cryptographic tools, including zero-knowledge proofs, homomorphic encryption, and cryptographic commitments. It explicitly prevents state agencies from classifying a developer or a protocol as a "money transmitter" or other regulated financial entity merely for creating or publishing privacy-preserving software. This pillar establishes a crucial safe harbor for innovation, allowing researchers and builders to work without fear of arbitrary regulatory reclassification.

2. Anti-Deplatforming and Anti-Blacklist Clauses:

The Act removes legal ambiguity by formally codifying the legality of core cryptographic tools, including zero-knowledge proofs, homomorphic encryption, and cryptographic commitments. It explicitly prevents state agencies from classifying a developer or a protocol as a "money transmitter" or other regulated financial entity merely for creating or publishing privacy-preserving software. This pillar establishes a crucial safe harbor for innovation, allowing researchers and builders to work without fear of arbitrary regulatory reclassification.

3. A Fundamental Right to On-Chain and Offl ine Privacy:

The Act affirms the fundamental right of all Texans to transact and conduct business privately, both online and in the physical world using privacy enhancing tools. It further recognizes that the use of cryptographic tools to ensure anonymity is a form of protected speech, shielding individuals who seek privacy from government intrusion, just as the law protects anonymous political or literary speech. It protects children from predators and stalking by moving sovereignty into theirs and their parents hands.

Hayden "Dax" Porter
dax@zeralabs.org

A Framework for Freedom:
The Seven Pillars of the Act [2/2]

4. Due Process Prior to Protocol Intervention:

This pillar establishes powerful due process protections, requiring state agencies to obtain a court order based on a high evidentiary standard before they can compel any action against a digital asset protocol. This includes mandating a backdoor, forcing a shutdown, or seizing control of its operation. It guarantees that technological systems are afforded the same rigorous legal protections as any other form of private property or enterprise.

5. A Regulatory Sandbox for Auditable Privacy:

Acknowledging the need to balance privacy with accountability, the Act creates the nation's fi rst "privacy protocol sandbox." This program provides legal clarity and safe harbor to innovators developing protocols that feature built-in, mathematically verifiable mechanisms for selective disclosure (such as ElGamal-Twist encryption). It incentivizes the creation of systems that are private by default but can comply with a lawful warrant, creating a clear pathway for compliant innovation.

6. Protections Against Extraterritorial Enforcement:

To defend Texas's sovereignty, this pillar bars state agencies from automatically enforcing federal rules or sanctions related to digital assets that have not been independently debated and adopted by the Texas Legislature. This ensures that the digital economic policy of Texas is set by Texans, for Texans, and prevents federal overreach from dictating the course of innovation within the state.

7. Technological and Economic Rights:

Finally, the Act guarantees the right of individuals and businesses to conduct unlimited private transactions, so long as they are compliant with Texas law. It explicitly protects the development and publication of privacy software, treating code as protected speech and a vital component of technological progress. This ensures that the next generation of financial innovation can be developed openly and freely within the state.

Hayden "Dax" Porter
dax@zeralabs.org

Conclusion:
A Critical Mandate for Texas

The Texas Privacy-First Digital Finance Act is not merely legislation about cryptocurrency or digital assets; **it is a foundational framework for securing individual liberty, economic prosperity, and personal security for all Texans** in the digital age. In an era of growing surveillance and regulatory ambiguity, this Act provides clear, principled, and predictable rules of the road.

By grounding these rules in the certainty of mathematics and the enduring principles of the Constitution, Texas can decisively reject the federal overreach seen in cases like Tornado Cash and instead champion a better path forward.

This legislation protects the right of every Texan to communicate, transact, and conduct business privately, free from unwarranted intrusion. It secures the rights of innovators to build the next generation of secure technology on Texas soil without fear of arbitrary enforcement. It treats computer code as speech and software developers as innovators, not liabilities, placing responsibility where it belongs: on those who misuse tools, not on those who create them.

The technical foundation for these systems has been proven. The economic opportunity - in investment, jobs, and tax revenue - is undeniable. The constitutional mandate to protect the rights of the people is sound. The choice before the Legislature is therefore a historic one: lead the world in defending digital privacy and economic freedom, or cede that essential role to others.

With this Act, Texas will not only become the global hub for privacy technology but will also send a clear message that the fundamental rights of its citizens extend to all frontiers, both physical and digital.

The time for Texas to lead is now.