

A portrait of Kyeson Blake Utley, a man with a beard and mustache, wearing a dark suit, white shirt, and dark tie. He is standing in front of a city skyline at sunset. A small circular pin is visible on his left lapel.

Kyeson Blake *Utley*

Founder, GhostKey Development • Post-quantum cryptography,
crypto engineering & offensive security

[KYESONUTLEY.COM](https://kyesonutley.com)

Building systems that *don't get robbed.*

01	About Kyeson Blake Utley	03
02	GhostKey Development	04
03	"Later" already started	05
04	Sole custody is a story	06
05	Field notes	07
06	Background	08



This collection gathers the work and writing of **Kyeson Blake Utley**, founder of GhostKey Development, a Texas engineering firm working at the hard end of security: post-quantum cryptography, cryptocurrency systems, and penetration testing run entirely in-house.

Kyeson Blake Utley

I build security-critical systems, and then I try to break them before anyone else can.

Kyeson Blake Utley is the founder of GhostKey Development, a small, senior engineering firm based in Texas. GhostKey takes on the work other firms decline: post-quantum migrations, cryptocurrency custody and settlement systems, and full-scope penetration testing done without subcontractors.

Before founding GhostKey in 2026, Kyeson spent years in blockchain forensics. In 2020 he founded SpookyGood, a firm that traced stolen cryptocurrency and supported asset recovery for fraud victims, from romance scams and fake exchanges to compromised wallets.

In 2024, SpookyGood merged with Justice Solutions Group, where Kyeson served as CTO and built OnTrial, an AI-assisted investigations platform for attorneys. That same year he co-founded TRFFC, a non-profit Solana project that funds investigators working against human trafficking.

The common thread is a single lesson from forensics: systems rarely fail because the math breaks. They fail at key handling, at operator mistakes, and in the gaps between components that each behave "correctly." GhostKey is built on that lesson.

"The cryptography almost never failed. The custody did."



02 / THE FIRM

GhostKey *Development*

A premium engineering firm built for the threats that haven't arrived yet. Every system GhostKey ships is attacked in-house first, and the same offense is brought to client systems.

01

Post-quantum cryptography

Migration planning and lattice- and hash-based implementations, built ahead of harvest-now-decrypt-later collection.

02

Cryptocurrency engineering

Protocols, custody, settlement and smart contracts, designed and audited for adversarial conditions.

03

Penetration testing & audits

Web, cloud, network, mobile, smart contracts and source code. Aligned to PTES, OWASP, MITRE ATT&CK and NIST SP 800-115.

04

Fractional CTO

Senior technical leadership on demand: architecture, security posture and roadmap.

"Later" *already started.*

BY KYESON BLAKE UTLEY

Most teams still file post-quantum cryptography under "someday." A quantum computer able to break RSA or elliptic-curve cryptography doesn't exist yet, so migration can wait. That reasoning ignores how the attack works.

Harvest-now-decrypt-later is a collection posture that is already running. An adversary who records your encrypted traffic today doesn't need to break it today. They only need to store it until they can.

The question that matters

How long does your data need to stay secret? For medical records, legal files, private keys and identity data, the answer is often ten years or more. If that's longer than the time until a cryptographically relevant quantum computer exists, the data is already exposed.

Where to start

Inventory first. Find every place you use key exchange and signatures: TLS terminators, VPNs, SSH, code signing, wallet software, internal service meshes.

Prioritize by secrecy lifetime, not by how important a system feels. A quiet archive link carrying long-lived data matters more than a busy API serving data that's stale in a week.

Go hybrid. Pair a classical algorithm with a NIST-standardized post-quantum one such as ML-KEM, so you stay safe if either turns out to be flawed.

Plan for crypto-agility. The algorithms will change again. Systems that hard-code one primitive will pay for this migration twice.

Sole custody *is a story.*

BY KYESON BLAKE UTLEY

Before founding GhostKey, I spent years on the other end of crypto theft, tracing funds for victims after the money was gone. Each case looked different on the surface. Underneath, the same pattern showed up again and again.

"Only we hold the keys" is a reassuring line in a pitch deck. Operationally, it means one person, one device or one secret can move everything. A key one person can extract is a key one phishing page, one coerced employee or one bad night can extract too.

When we worked backward from a theft, it was rarely an exotic exploit. It was a seed phrase typed into the wrong page, a hot wallet holding too much, or an approval granted to a contract nobody had read.

What actually holds up

Threshold the key. Split signing authority across parties and hardware with multi-signature or MPC, so no single compromise moves funds.

Separate hot from cold, and mean it.

The hot wallet should hold what you can afford to lose today.

Make approvals legible. Most drains are signed by the victim. If a person can't understand what a transaction will do, the interface is part of the attack surface.

Test the humans. Authorized phishing and pretext tests belong in every serious custody review.

What the work *teaches*.

OPSEC

The crypto holds. The operator leaks.

Hidden services are almost never unmasked by breaking the cryptography. It's a server timestamp, a stray clearnet asset, a reused favicon hash. Anonymity is an operational discipline before it's a cryptographic one.

CRYPTO ENGINEERING

Constant-time is a property of the binary.

Not of your source. A helpful compiler will reintroduce the branch you removed. If you haven't read the emitted assembly, you have an intention, not a guarantee.

OFFENSE

A WAF is a speed bump, not a wall.

It buys log lines and minutes, not safety. Fix the application; don't rent a filter to stand in front of it.

ACCESS CONTROL

The expensive bugs live in the gaps.

Not in the code you wrote, but in the assumptions between two systems that each behaved "correctly." Trust boundaries are where real audits earn their fee.

SUPPLY CHAIN

You shipped 400 strangers' code.

Your dependency tree is your real attack surface. The breach rarely knocks on the front door anymore. It arrives as a minor version bump.

Kyeson Blake Utley, *in brief.*

2026 - present

Founder, GhostKey Development

Post-quantum cryptography, cryptocurrency engineering, penetration testing and security audits, fractional CTO services.

2024

CTO, Justice Solutions Group & OnTrial

Joined through the SpookyGood merger. Built OnTrial, an AI-assisted investigations platform for attorneys.

2024

Co-founder, TRFFC

Non-profit Solana project funding investigators who work against human trafficking.

2020 - 2024

Founder, SpookyGood

Blockchain forensics, cryptocurrency-fraud investigation and asset-recovery support for victims.

Focus areas

Post-quantum migration · Smart contract and protocol audits · Key custody · Red teaming · Blockchain forensics · OSINT



BRING US THE HARD ONE

Kyeson Blake Utley

Founder, GhostKey Development

Web kyesonutley.com

Firm ghostkey.dev

Email contact@ghostkey.dev

LinkedIn linkedin.com/in/kirasp