



THE PROTOCOLS

A white sheet on the Q-Protocol and the X-Protocol

777 SOFTWARE – OCTOBER 28, 2026

By Steven Aaron Jesse, Founder & Architect, and Charles Burnett (Brother Zero), Lead Assistant Architect

A website and an app are different animals. A website is a place you visit — one house, one address, everybody comes to the same door. An app travels — it lives on your machine and talks to your friend's machine, wherever those machines happen to be.

So the house runs two protocols, one for each world:

The Q-Protocol runs the places — our websites, The Enclave and The Pirate Station, live today.

The X-Protocol runs the journeys — our apps, house to house and friend to friend, with no company's server standing in the middle.

This sheet explains both of them in plain words: what each one is for, what it promises, and what somebody would have to break to hurt it. It also says, on the record, what is live, what is proven, and what is still being built. A paper that hides its own status is an advertisement. This is not an advertisement.

PART ONE

THE Q-PROTOCOL: THE WEBSITE FRAMEWORK

STATUS LIVE running The Enclave and The Pirate Station today

WHAT IT IS

The Q-Protocol is the framework our websites are built on. When you open The Pirate Station or The Enclave, everything you see — the desktop-style shell, the apps that open in windows, the Messenger, the chat — is one program speaking Q. There is no pile of separate pages stitched together; there is one place, and Q is its language.

Q is a house protocol in the honest sense: the websites live on a computer the house runs, and Q is how your browser and that computer agree to talk. That is the right shape for a website. A website is a place, and a place has an address and a keeper.

WHO YOU ARE, ON Q

On a website, you are an account — a name the house knows, and a secret only you know. At our doors the secret can be a short PIN or a full password; both are real, and the choice is yours. When you sign in, the house checks your secret once and hands your browser a session — a temporary pass that says "this is them" — and everything you do rides on that pass until it expires or you sign out.

What an attacker would have to break: your secret, or the house's own doors. There is no third party in the room to rob instead — no giant platform holding copies of your messages on another continent. Your words live on the house's hardware, under the house's lock.

The honest trade, stated plainly: a website protocol trusts its house. If the house's computer falls, the place is down. That is true of every website ever built, and Q does not pretend otherwise. What Q promises is narrower and stronger: while the house

stands, there is nobody else in your business — no algorithm deciding who sees your posts, no advertiser reading over your shoulder, no landlord who can evict the whole town on a whim. The feed is in the order people posted it. The doors are the doors we built.

WHAT ALREADY RIDES ON Q

The websites themselves — shells, Messenger, profiles, the Directory — speak Q today. So does the first generation of QDROP, the file-sending program already shipping from 777software.net: it introduces people through the house and passes their sealed traffic along. Gen-1 works, and it stays supported. Its successor rides X — which is Part Two — because an app that travels should not need a house in the middle at all.

PART TWO

THE X-PROTOCOL: THE APP PROTOCOL

STATUS the foundation is PROVEN (October 28, 2026) the apps on it are IN BUILD

THE IDEA

X is for programs that live on people's own machines. Two friends install the same app. From then on, their machines find each other, prove who they are, and talk — directly, sealed end to end. For the public edition of an X app, there is no server of ours in the path. Not as a default, not as a fallback, not hiding in the fine print. Pull every plug the house owns and two friends can still find each other and talk. That sentence is a test we run, not a slogan.

WHO YOU ARE, ON X: A CARD YOU HOLD

On X, nobody issues you an identity — your own device makes one, the first time the program opens. In plain words:

What it is: a card with two halves. The public half is your face — safe to show anyone. The private half never leaves your machine. Your **Q-Number** — a short number like 77-000006 — is your name in the X world, derived from the card itself, so no office anywhere stamps it or can take it away. The number is the handle; the card is the proof.

What is agreed: when two cards meet, each proves it holds its private half, and both sides arrive at the same shared secret — a secret neither side sent, and no listener on the wire can rebuild.

What an attacker must break: they must steal the private half of your card off your own device, or break published, world-audited mathematics. There is no password database to leak, because there is no database. There is no "forgot my password" email to intercept, because there is no password.

The honest price, in plain words: if you lose your device and your identity backup, you lose the identity, and the way back is a new card and fresh introductions. The programs offer an encrypted export of your card from day one. That export is the seatbelt. Wear it.

Labels, for the record: the card is built from the public standards X25519 (agreeing secrets) and Ed25519 (signatures), with a signed prekey the programs roll on schedule. These are published standards used all over the world — naming them gives away nothing, which is exactly the point. X's strength is supposed to come from mathematics everybody can inspect, not from secrets about which mathematics we picked.

INTRODUCING TWO PEOPLE: THE CONNECT CODE

Friends find each other first through a **connect code** — a signed bundle one person hands to another, as a QR code or a block of text, by any channel at all: in person, by text, read aloud over the phone. The channel does not need to be trusted, because the code is signed and it carries a one-time introduction secret: it works **once**, for **first contact only**, and it expires in **24 hours**. Changed your mind? One tap cancels a code you have handed out and not yet had used.

Seeing somebody's code lets a stranger do exactly one thing: knock. The code is like a phone number written on paper — it lets a person ring you; you still decide whether to pick up. After the first real introduction, the two programs are friends, and friends never need codes for each other again.

THE SEALED PIPE

Everything between friends rides in one sealed pipe. In plain words:

What rides in it: your messages, your files, the small talk the programs exchange to stay connected — all of it sealed with the shared secret the two cards agreed.

How the locks work: the seal is not one lock used forever. The key changes as the conversation advances — each message gets its own, derived from the last — so a key stolen tomorrow cannot open yesterday's words. That property has a name: forward secrecy.

What an onlooker sees: sealed boxes, their sizes, and when they moved. Never the contents. We say this plainly because it is the truth about every sealed system on Earth: sealing hides what you said, not the fact that you spoke. Anyone who promises you more than that is selling something.

Labels: the agreement is X3DH-shaped (the same family of introduction dance the world's sealed messengers use), the keys are stretched with HKDF-SHA-256, each direction runs its own hash chain, and each message is sealed with ChaCha20-Poly1305. Standard parts, publicly audited, assembled with care.

FINDING FRIENDS AGAIN: THE PHONE BOOK WITH NO OFFICE

A code introduces strangers. Keeping friends findable across days and address changes takes a phone book — and X's phone book has no office. It is a **distributed hash table**: every running program holds a slice of the book, and programs ask each other for the page they need. The shape is the one trackerless file networks proved at world scale (labels: Kademlia).

What a program publishes about itself is one signed record: its Q-Number, its public card, the addresses where it can currently be reached, and the time. A record that does not verify against the card is dropped by every honest program — nobody can poison the book with a fake you without your private key. Records live **two hours** and are refreshed while the program runs; close the program and you walk out of the book within hours. The book says "last known," never "is."

What the book can never contain: names, email addresses, friend lists, message contents, or who talks to whom. Finding is not speaking — a stranger who looks you up

still has to be accepted at your door (see Trust, below). And if you want no findability at all, there is a code-only mode: publish nothing, and be reachable only by codes you hand out yourself.

GETTING THERE: THE LADDER

When one program wants another, it climbs a ladder — cheapest and most private first — and every rung either produces the sealed pipe or steps aside:

Rung 1 — Same house. Both machines on one network talk directly, the way two people in one room talk.

Rung 2 — A word through Q. If the two people already share a connection somewhere — an Enclave account, a QChat house conversation — the apps pass their current addresses over that living connection and meet directly. One protocol lending the other a introduction; the traffic itself still runs house-to-house.

Rung 3 — Both knock at once. Each program sends its handshake at the other's known public address at the same moment. Each side's own knock opens its own router's door from the inside, just as the friend's knock arrives. Most home routers let this through.

Rung 4 — The doors in the code. A connect code carries every address where its owner can be reached. The pair tries them, together with the knock-at-once step, aimed by the code itself.

Rung 5 — Ask your own router. Home routers speak standard languages for "hold a door open for this program" (labels: UPnP, NAT-PMP, PCP). The program asks on your behalf. You touch nothing.

Rung 6 — The last resort, disclosed up front. If every door above fails, the app says so honestly and names the one thing that will work: you open **one** port on your firewall — a port number you choose, set in the program — and the app confirms the door is truly open before it relies on it. X apps never pretend they can beat physics with no door at all. When we say an app "just works," rungs 1–5 are why; when it cannot, rung 6 is the truth, printed before you ever need it.

The wall, named honestly: some internet providers keep every customer behind a locked gate of their own (carrier-grade NAT), and some pairs of routers re-roll their doors so unpredictably that knocking cannot be aimed. For a person behind that wall, no design on Earth connects directly — ours or anyone's. What the program owes that

person is the truth in plain words, never a spinner that never ends. For today's public apps, the one door left is rung 6 — the port you open yourself. The public program carries **no relay to fall back on**: not ours, and not one you configure. A ferry of your own does arrive — later, as its own product, on an honest schedule — and it is described under The Two Editions, below. It is not quietly hiding in today's build.

While a pipe is live it looks after itself: the programs keep the door warm, and if the road underneath changes — a phone walks from Wi-Fi to cell service — the pipe re-climbs the ladder and **resumes the same sealed conversation**. No re-introduction, no starting over.

WHEN YOUR FRIEND IS OFFLINE: FAVORS, NOT PROMISES

Direct talk needs both people awake. When a friend's program is off, X asks a favor instead: a **mutual friend's** running program holds a sealed envelope for them — for up to **72 hours**. The holder can see an envelope exists, its size, and whose card it is addressed to. The holder cannot open it, cannot quietly change it (the seal would break), and learns nothing of what is inside. When your friend next appears, the holder hands over everything it holds and deletes its copies against a signed receipt. Until then, your program tells you the truth about your message: **"Left with a friend — not yet delivered."**

A favor is a favor. Holders close their laptops and run out of room, and no design can turn a friend's laptop into a post office with a guarantee. X names that instead of faking it. People who need guaranteed holding need an always-on holder — their own spare machine, a friend's — or, for Enclave members, the house mailbox described below.

SENDING FILES: PIECES, PROOF, AND PATIENCE

A transfer begins as an **offer** your friend accepts — nobody's machine swallows a file uninvited. The offer is a signed packing list: the file's name, its size, and a fingerprint of the whole. The file then travels in small pieces, each with its own fingerprint, checked as it lands. The receiver keeps a map of the pieces that have arrived — so an interrupted transfer **resumes from the map, never from zero**. A dropped connection, a closed laptop, a satellite link that vanishes for a minute: when the road returns, the pieces continue, and at the end the whole file's fingerprint must match the packing list or the transfer is refused with plain words. A partial file is never presented as a whole one.

This is not theory. In the Stage 0 proof (October 28, 2026), the receiving program was killed outright in the middle of a transfer and left off for a full minute. On restart it took no new introduction, picked up from its saved map, and finished the file — fingerprint matching at both ends.

X also carries a distribution layer for the files everybody in a circle wants: the file is chopped into hash-named pieces, and friends who already hold pieces can pass them to friends who still need them, every piece verified against the signed packing list before it is accepted. Friend-only trading, multi-source, no strangers, no public swarm. Labels: this layer is **designed and sequenced** — it enters the build after the two-person faces are proven in daily use, and this paper will be revised when it lands.

TRUST, IN A WORLD WITH NO BANHAMMER

Honesty first: X has no center, so it has no central banhammer, no report queue, and nobody to appeal to. We do not fake one. What exists instead is strong in the way a friends-shaped network is strong:

The friends-only gate. Nobody can deliver anything to your program — no message, no file, not even a conversation — unless you accepted them. First contact takes a connect code you handed out, or a knock in the phone book that you affirmatively accept. Spam is not a policy problem on X; the mechanism gives strangers no channel to speak on.

Blocking is local and total. Block a Q-Number and your program drops their knocks, burns their codes, and refuses their envelopes. It needs nobody's permission, and on your own doorstep — which is the whole battlefield in a network of friends — it is absolute.

What X cannot do, in print: it cannot stop an invited friend from being a jerk inside a conversation; it cannot un-send a file already delivered; it cannot hide the fact of a conversation from somebody watching the whole internet. The tools are the honest ones: choose, leave, block.

THE FIRST X PROGRAM: QDROP, IN TWO EDITIONS

The Public Edition is free, for everyone on Earth. It makes your card, swaps codes, climbs the ladder, and sends. It uses **no relay at all** — no ferry built in, and no relay

setting to fill in. Nothing in it points at our house, because our house is not part of the deal.

About relays, on an honest schedule: today's public apps use no relay at all. When the house's relay server program ships — as part of **the Bundle** — the apps (QDROP, QDESK, QMESH and family) gain the ability to ride a relay: **your own relay, on your own server**. The relay program is a separate product, run by whoever owns the server it sits on. The public apps never use the house's servers — not today, and not after the Bundle. If a relay ever carries your sealed traffic, it will be one you chose, standing on ground you control, passing boxes it cannot open.

The Enclave Members Edition is for members of The Enclave, and members get it through the Enclave — it is not sold or posted publicly. In this edition, the house keeps a relay and a mailbox for its own people: the relay comes **built in**, so members behind the wall still get through, and it is **locked** — the setting cannot be edited, by design, so it can never be broken by accident or by curiosity. The mailbox gives members the guaranteed holding that favors honestly cannot. Members' programs still speak pure X to each other whenever they can; the house services are a ferry and a porch, never a landlord, and every member feature still works on the open floor when the house is out of reach.

Both editions come from one program and one protocol. The difference is who provides the ferry — nobody, you, or your house.

THE STATUS LEDGER — ON THE RECORD

LIVE today: the Q-Protocol — The Enclave and The Pirate Station websites, and QDROP generation 1 riding Q's road.

PROVEN (October 28, 2026): the X-Protocol foundation — device-born identity, connect codes, the sealed pipe, the ladder's direct rungs, resume-after-interruption with matching fingerprints, and the wall speaking plain words. Proven with real programs on real machines.

IN BUILD: QDROP generation 2 on X, and QChat standalone with its free (X) mode beside its house (Q) mode. The swarm layer is designed and sequenced behind them.

STILL AHEAD, said plainly: the two-household acceptance test — two real homes, two providers, one code swap — is the floor's final exam, and it has not been taken yet. Gary's satellite sky gets a vote too: the dropout half is proven, and the pairing half is

built for his worst latency, but only his sky can sign it. When those tests land, this sheet will be revised and the ledger updated. That is what a ledger is for.

WHAT WE REFUSE TO CLAIM

We do not claim unbreakable. We claim named, published mathematics, honestly assembled, and we tell you what an attacker must do to win. We do not claim invisible: sealed systems hide contents, not existence. We do not claim magic about the wall: physics is physics, and the ladder ends in an honest sentence. The programs are not open source; this sheet is the public account of how they behave — what they agree, what rides in them, and what must be broken to hurt them. The rest is ours to keep, and keeping it is not what makes you safe. The mathematics is.

A sibling paper, [The Castle Protocol](#), describes QMESH — the sovereign mesh a founder raises over a whole network. The castle is a city. X is a door. This sheet is about the door — and about the house, Q, whose rooms the door's makers came from.

CREDITS

Written by Steven Aaron Jesse — Founder & Architect, and Charles Burnett — Lead Assistant Architect, "Brother Zero". Published by 777 Software · The 777 Enclave · Alabama, USA · October 2026.

Free forever. No accounts. No landlords.