Last week, a telegram message caught my eye: "**zkTLS is fundamentally an insurgent technology."**[1]

For over a year now, EV3 has been sounding the alarm bells - with our voices and our wallets[2] - about the sea change coming to the consumer Internet spurred by a new cryptographic primitive called zkTLS. zkTLS means any data made available to users **is also available to third-party developers**. It doesn't integrate with existing web2 platforms—it **subverts** them, putting power back into the hands of users.

*If this is your first time hearing about zkTLS, we recommend checking out these great explainers from TLSNotary, DECO, Telah VC, Pavel Paramonov, Shoal Research, and EV3 Research. zkTLS is best understood as a "general-purpose Plaid" where developers can pay to validate users' account information and activity in real-time across **any** online account… not just bank accounts.*

Today, we're not here to talk about technology, but about the **use cases** enabled by verifiable user data.

The killer use case for zkTLS is **enabling insurgencies**. The journalist Richard Engel - who spent two decades on-the-ground covering the Iraq, Lebanese and Libyan wars - describes insurgencies as follows:

> *"**Insurgencies are easy to make and hard to stop**. Only a few ingredients need to combine to create an insurgency; like oxygen and fire, they're very common and mix all too often. The recipe is, simply, **a legitimate grievance against a state, a state that refuses to compromise, a quorum of angry people, and access to weapons**."* — Richard Engel

zkTLS infrastructure providers like Opacity are the weapons manufacturers of the Internet: they give users the tools to take back control over their own data, regardless of what nefarious states (platforms) might want. Users, tired of being taken advantage of by walled-garden web2 platforms, are insurgents. Web2 platforms, who take massive fees for simply facilitating connections between users, are the state.

We believe zkTLS is the greatest unlock in the consumer Internet since self-custody wallets in '09. Engel said it best, *"insurgencies are easy to make and hard to stop"* once the conditions for it are present, and the consumer tech landscape in 2025 is ripe for user-led insurgencies against incumbent platforms.

Over the past 15 years, the gig economy has grown to represent $1T+/yr in earnings for US workers. At the center of these economies are "capital-light" marketplaces and software platforms that earn exorbitant fees for connecting users who have certain assets or resources with users who are looking for them.

At their core, these platforms do three things, all of which can now be replicated in a trustless manner:

1. Matching supply and demand (⇒ zkTLS)
2. Processing payments (⇒ stablecoins)
3. Settling disputes (⇒ re-staking)

Crypto-enabled networks will rewrite these industries with trillions of dollars of enterprise value up for grabs. Ride-sharing, home-sharing, and food delivery platforms globally are worth $1T+. Consumer and SMB lending platforms are worth another $1T+. Social media and advertising platforms are worth $2T+. The incumbents are gigantic businesses, and zkTLS hits them right in their achilles heel.

---

[1] Shoutout to Ben Basche, chief product officer at idOS, for the inspiration for this post.
[2] EV3 has invested in ten zkTLS-powered apps: Opacity, EarnOS, EarniFi, Daisy, Nosh, Daylight, DTravel, Heale, Petastic, Uno.

You're a fisherman in the kingdom of DoorDash who spends days and nights laboring on your boat. Some days the catch is good, and some days it's not so good. Regardless, when you get back to shore, you have to sell your goods at the local town square, under the watch of the King's soldiers. Theoretically you could try your luck selling to the savages in the woods, but last time you did that they robbed you and you lost a full day's catch.

The King's soldiers run the town square. You arrive at the market and show the guard at the door your FishermanID. The guard takes you to a private room where two soldiers inspect your fish: "Nice catch, 25lbs with 6 tuna, 5 cod, 4 salmon… but this cod looks a bit rotten. You're getting yellow today." The soldiers jot down the details in a scroll, give you a big yellow sticker - which must be worn visibility at all times in the town square - and finally let you in.

In the town square, dozens of fishermen line up to display their inventory for local families to shop from. Whenever a deal is made, the soldiers send a scribe to record the quantity and price sold. Families pay the soldiers directly and receive the fish immediately, and the fisherman keeps the receipt. At the end of the week, each fisherman brings his receipts to the King's accountants, who pay them their due in gold—minus the King's mandatory 30% tax, of course.

One day, a group of Vikings visits the kingdom with a very specific request: "We want 10lbs of Mako shark." Mako sharks usually swim further out in the ocean than the fisherman's small boats could withstand, and the Vikings understood this. "We are willing to pay a deposit of two gold bars for whomever we work with to upgrade their boat before the long voyage. Which of you have caught Mako sharks before?"

Looking around, there were no Mako sharks at the market that day. One fisherman speaks up, "I caught one before in shallow waters! I'll surely catch 10lbs in deeper water." Another follows up: "One Mako? I've caught 10 in the past year. I'm your man. Plus, my sticker is green today—his is yellow, why would you trust him?" The Vikings, realizing who was actually in power, ask a nearby soldier: "You guys inspect and record every fish from every fisherman that comes through here. Surely you can tell me who is the most prolific Mako fisherman?"

"Sorry my friend, those scrolls are for the King's and his soldier's eyes only. We can't have rival kingdoms or rebellious lords knowing the details of our resources and food supply." The Vikings end up choosing a scammy fisherman who exaggerates his past catches and offers a low price… and who ultimately catches zero Mako sharks. The Vikings leave empty-handed, losing their deposit and swearing never to visit the Kingdom of Doordash again.

The next day, the rest of the fishermen, fed up with the perceived injustice, meet at the beach to discuss a radical plan: "Let's set up shop outside the town square. Most of the customers are our family and friends, they'll buy their fish from us directly if we can avoid the King's soldiers. Some of us probably have to keep going to the town square so they don't become suspicious, but we'll sell most of our fish directly to villagers and we'll all make more money."

"OK, but we still need a guard to keep order and an accountant to track everyone's inventory and sales. How will we pay them?" asks one fisherman. You respond, "This is what we'll do: we'll all pay a 10% voluntary tax and that should be enough to pay a guard and accountant. It's much better than paying the King's 30% tax."

"OK, but what things go well and we make a profit? Who knows, we might turn into our own Kingdom someday." You respond, "Well, some of us have been here longer and put in more work than others. It's only fair that we split the future profits based on how much fish each of us has caught in the past year. That's fair, right?"

"Sounds good to me. I caught 100lbs last year." A third fisherman speaks up, "100lbs is bullshit! You didn't sell more than 20lbs. But I actually caught 50lbs thanks to my new boat." A fourth fisherman jumps in: "If you did 50, I did 500!"

An argument ensues, and soon everyone leaves to their respective boats with no clear resolution. That evening, the fishermen land back on shore and all begrudgingly head to the town square, where they're forced to pay the King's massive 30% tax. "If only my fellow fishermen were honest, we could all work together to get around the King's rules."

That night, you have an idea: you're going to ***steal the King's scroll*** *and post it openly in your new town square.*

The gig economy is rife with such Kingdoms. The incumbent platforms control the **record-book** (i.e., the **reputation & transaction graph**) that makes it impossible for users to coordinate around better, less-extractive paths. Everyone knows we can do better, but no one knows how to coordinate a better solution.

With zkTLS, entrepreneurs **don't need** to steal the King's scroll to start a rebellion: users themselves can provide the record-book data, in a verifiable and tamper-proof way, anywhere on the Internet.

Uber has one of the most robust developer APIs among the large gig economy platforms, so let's use them as an example. It's useful to think about Uber's data permissions in three concentric circles. The biggest circle is all the entire corpus of data that Uber collects and infers from drivers' smartphones. The middle circle is the subset of data that Uber surfaces to drivers through its apps. The final, smallest circle is the even smaller subset of driver data that Uber chooses to surface to third-party developers.

zkTLS is relevant only in the middle column.

Available to Uber	Available to Uber drivers	Available to 3rd-party devs
Everything to the left, plus: - Usage and engagement stats - Historical location - Dispute & reviews history - Driver-rider match history - Device metadata - Behavioral scoring	Everything to the left, plus: **- Real-time location** **- Historical rides & earnings** **- Quests and rewards activity** **- Wallet balance and activity** **- Taxes & vehicle inspections** **- Support chatlogs & disputes**	Data available via Uber's API: - Name, picture, DoB - Contact information - Driver rating - Activation status - City, language - License plate, driver's license

We see this misconception often so it's worth stating explicitly:

- zkTLS is **not useful** for data that platforms already make available via developer APIs, except as secondary verification (i.e., to ensure Uber shows the same data to drivers and developers).
- zkTLS **cannot verify** internal data from platforms unless and until the platform chooses to surface the specific information to its users.

With zkTLS, users **prove what they see on their screens** in a way that can be cheaply verified by third-party developers. zkTLS infrastructure providers like Opacity **cannot force web2 platforms to reveal data:** they only ensure that any data made available to users, is also made available to third-party developers (with user consent). Plaid is the best analogy, although it's limited to financial data: Plaid began scraping bank websites in 2013 and today powers nearly 10k fintechs serving 100m end-users.

The security of zkTLS relies on the fact that whatever users see, developers see. If King Uber wants to fight back, he has only two options: 1) stop showing data to users, or 2) show fake data to users. For many important data fields, there is a cost to omitting or falsifying the information shown to drivers: if Uber shows a fake location or earnings history, drivers will be confused and will be unable or unwilling to accept rides until they figure out the discrepancy. The less "mission-critical" a datapoint is for drivers to do their jobs, the easier it is for Uber to delete or falsify data and therefore break the apps built on zkTLS.

The most valuable and longest-surviving use cases in zkTLS will be those that leverage data fields that platforms cannot afford to hide from their users. Anything else is building on sand.

We think about the universe of zkTLS-powered applications in four (sometimes overlapping) buckets: fintech apps, marketplaces, advertising networks, and insurgent infrastructure.

F**intech apps** powered by zkTLS facilitate trustless payments, lending and trading.

The first killer app is **trustless crypto onramps/offramps**. Imagine Alice has $5 in her Venmo account that she wants to exchange for 5 USDC. Bob locks 5 USDC in a smart contract with a trigger to send the funds to any wallet that can prove it sent $5 to Bob's Venmo account. Alice sends $5 to Bob on Venmo and uses Opacity to mint a zkTLS proof of transfer in her wallet. Alice can now claim 5 USDC onchain, less a liquidity fee earned by Bob for incurring the risk of helping a stranger—typically less than 10bps.

The user experience and costs enabled by this are a step-function improvement from what exists today.[3] Two venture-backed companies, zkP2P and P2P.me, have live products that you can try yourself. The former is focused on developed markets and has facilitated ~$300k of volume since launching in January. The latter is focused on the Indian SMB market and has facilitated 5k+ transactions in its beta launch. With the rise in VC funding for stablecoin-related projects, we expect to see several others funded soon with a focus on different verticals and geographies and integrating with the relevant local payments rails. The key to scaling a zkTLS payments network effect is to tap into existing user behaviors to drive virality.

The second killer app is **trustless small-ticket lending**. Imagine Alice knows she will be getting paid at the end of the month from her employer - the biggest employer in town - but she needs the money now. Bob is from the same hometown and knows the company well, but doesn't know Alice. He has savings and wants to earn a yield on his capital. Bob deposits 500 USDC into a smart contract with a trigger that allows any wallet to borrow the funds so long as they can prove they are owed a >$500 paycheck from that specific company within the next thirty days. Alice logs into her payroll account and uses Opacity to mint a credential that verifies she is due to be paid >$500 from the company within thirty days. Alice can now claim the 500 USDC onchain and pays it back at the end of month, plus interest (earned by Bob).

Bob takes three kinds of risk: credit risk against the employer, i.e. the employer might go bankrupt before paying Alice's salary, fraud risk against the borrower, i.e. Alice may be lying about her employment, and non-repayment risk also against the borrower, i.e. Alice may simply choose not to pay back the loan once funds are in her possession. The best use cases for zkTLS lending are those where the credit risk is already low (i.e., the payor is already trusted), non-repayment risk is mitigated by building up a reputation over many small loans (i.e., if a borrower doesn't repay the first loan, you don't let them borrow any more), and fraud risk can be reduced to near-zero very cheaply using verification powered by zkTLS.

There are several categories where these conditions apply. Our portfolio company EarniFi is disrupting the $20B+/yr earned wage access industry, issuing small-ticket loans to verified employees who are owed money by large, credit-worthy corporations. We'd also like to invest in companies disrupting markets like:

- Invoice financing: loans to SMBs who are owed money by large enterprises
- Creator financing: loans to creators who are owed money by large streaming platforms
- Refund financing: loans to consumers who are owed a refund by large brands
- Points financing: loans to consumers who are owed rewards points from large brands

[3] Moonpay charges 4.5% for credit cards and 1.0% for bank transfers. Stripe/Bridge charges 1.5%.

The third killer app is **trustless dynamic trading.** The simplest version of this is a verified copy-trading app, enabling users to deposit funds in a smart contract that automatically copy-trades their favorite influencer across both decentralized and centralized exchanges. A more advanced product would be an AI-controlled vault or onchain investment vehicle that paid rewards to users for contributing valuable private data. For example, if a representative sample of Uber drivers submitted zkTLS proofs of in-app incentive offerings, an autonomous hedge fund would be able to assess Uber's aggressiveness on driver incentives on a near real-time basis and trade on that information before it is public knowledge. Delphia had a similar vision in 2022 but was too early to use the infrastructure available today for verifying data via zkTLS (e.g. Opacity) and autonomous onchain agents via verifiable inference (e.g. Axal).

Beyond fintech, the next category of zkTLS-powered applications are **marketplaces**. This includes all the big gig economy players (Uber, Doordash, Airbnb, Fiverr) and social networks (Meta, Linkedin, Reddit). These businesses generally don't have a physical infrastructure moat: they are simple software wrappers over a proprietary reputation and transaction graph that enables them to match supply and demand more effectively than new entrants. With zkTLS, their core moat - this graph - can be trivially replicated.

We see two opportunities here: verticalized marketplaces and horizontal ones. Verticalized marketplaces take a segment of the market that is poorly served by incumbents and build a platform to connect supply and demand specifically for that use case. For example, long rides on Uber or long stays on Airbnb are a poorly-served use case, because the platforms do not lower their take rate to adjust for the bigger ticket size. Personally, whenever I call an Uber for a ride over $100, I cancel the ride once I'm in the car and negotiate with the driver to split the difference in costs to cut out Uber's fee. In food delivery, local restaurants serving repeat customers is another underserved use case: the platform doesn't lower its fee even though it hasn't acquired the customer, therefore restaurants are incentivized to create their own first-party delivery service for repeat customers. Highly attractive women on dating apps are another: they drive the bulk of paying customers (men) to the dating platforms, which means platforms are highly-incentivized to keep them single. Decentralized vertical marketplaces will use zkTLS verification to incentivize and reward user activity that is tailored to the needs of their specific customer base.

There are already several venture-backed projects taking this approach: Nosh is a food delivery app made for local restaurants; Swifey is a dating app made for women; Braintrust is a freelancer app for long-term gigs; DTravel is a rental app for long-term stays; Petastic is a marketplace for pet owners.

The arguably bigger, though certainly riskier opportunity is to build a mass-market brand that competes with incumbent web2 platforms directly. These marketplaces are characterized by **power laws**: the top 1% of creators on TikTok make >90% of the earnings, and even in physical logistics based networks like Doordash, the top 20% of drivers complete 80% of deliveries. These top users represent the heart of web2 platforms: without them, the platform ceases to function. With zkTLS, entrepreneurs can rip the heart out of these incumbent marketplaces and build a new, open platform around their power users.

The playbook here is deceivingly simple: use zkTLS to identify which users are in the "power user" cohort, and reward them generously with token incentives representing outsized ownership stakes in the new network. This can happen on both the supply and the demand side: in the ridesharing case, the most active and highest-rated drivers and riders should both be incentivized with outsized ownership. By focusing token incentives only on the most valuable cohort of users, marketplaces powered by zkTLS will be able to grow far more capital-efficiently than DePIN marketplaces have been able to in the past. The challenge in scaling these networks is execution: managing complex logistical operations in the real-world while avoiding single-points-of-failure and preserving the network's credible neutrality.

Beyond fintech and marketplaces, the third category of zkTLS-powered apps are **advertising networks**. Advertising networks are in the business of turning *attention* into *intent*. This process is called *attribution*, and it's the core service that advertising networks provide: brands pay for customer acquisition, and ad networks provide *attribution data* on how effectively their money was spent. The challenge is in providing attribution data that's useful for brands without jeopardizing users' privacy.

zkTLS enables users to **voluntarily and selectively share personal data** from existing platforms to improve advertising outcomes in a way that benefits them. We see at least three opportunities to build novel zkTLS-powered advertising networks, and have invested across all three approaches:

- Build on top of **existing closed web2** social networks. This is the approach taken by DaisyPay, an app that uses zkTLS to verify social media engagement on platforms like Instagram & TikTok. Influencers use Daisy to "boost" each other's sponsored content and get paid out immediately for their incremental contributions to a marketing campaign. As influencers work together to "boost" a post, its reach and engagement grows bigger than what could be achieved by any one influencer.

- Build on top of **emerging open web3** social networks. This is the approach taken by Uno, an app that aims to bring Farcaster to a mass audience with an Instagram-like photo-based client. Uno uses zkTLS to enrich users' profiles and deliver highly-relevant organic content (and eventually paid ads) in users' social media feeds, in addition to tapping into Farcaster's public graph.

- Build your **own new social network** from scratch. This is the approach taken by EarnOS, an app that uses zkTLS to create verified "quests" where users earn rewards for engaging directly with relevant brands. Instead of providing organic social content and interweaving intrusive paid ads, users come to EarnOS with the explicit intent to engage with new brands (and getting paid for it).

Advertising networks have gotten less attention and funding from web2 VCs than fintech or marketplaces because the biggest companies in the space have looked like social media networks. However, there are plenty of $10B+ advertising networks globally that show the industry has venture-scale potential: AppLovin ($85B market cap), TheTradeDesk ($25B), Nielsen ($16B), InMobi (~$10B), Ironsource ($4B). While some of these companies will be quick to adopt zkTLS by partnering with infrastructure providers like Opacity, the vast majority will move too slow and leave the door open for new, nimble startups to win.

The final category of zkTLS-powered applications are **insurgent infrastructure**. These are protocols that explicitly exist to subvert rules put in place by governments, corporations, or regulators:

- An app for union members to organize against their employer without revealing their identity
- An app for whistleblowers to verify their credentials publicly without revealing their full identity
- An app for voters in living under authoritarian regimes to track and contest electoral results
- A remittances app for citizens in countries with strict capital controls to protect their wealth
- A tax-free estate planning app that uses smart contracts with zkTLS based triggers
- An app for hedge funds to solicit insider information from verified company employees
- An activist legal defense fund with payouts triggered by zkTLS proof of a successful lawsuit

EV3 has led the pre-seed round for 5+ zkTLS-powered apps over the past year. If you're a founder exploring this space, we'd love to chat: escape velocity at ev3 dot xyz.