ZK Proofs: Chasing Problems That Don't Exist?

Vladislav Solodkiy
Founder & ex-CEO @ ArivalBank.com, a.id, SREDA.VC I Early investor in 5 digital banks

April 15, 2024

Is ZK proof a solution looking for a problem that doesn't exist? World and other digital identity startups are heavily betting on and discussing "zero-knowledge data transfer" – but is there really a demand or a client for this pain? 'Optimization' can be harmful **without a real 'Client' with a real 'Problem' – improvement alone isn't enough motivation**. In blockchain and crypto, there are too many programmers and engineers and not enough product owners, as for me. There's too much talk about "let's make the technology even more perfect," and not enough about "who is our customer and what problem are we solving?"

Meyer "Micky" Malka 's Ribbit Capital added here: "When we step back, we see a good chance that central identity problems – for example, "how can I provide KYC-level information (e.g. proof of address, age verification), re use it with multiple parties, and comply with regulation – and do it all without divulging the underlying data (e.g. home address or birthdate)" – are more likely to be solved first in crypto."

Roughly speaking, "*trust but verify*" is a good point – every member of the community or state can, or even should, *double-check* their community, company, state, *rather than blindly trust it*. Ok, I will repeat this again and again – who is the Client here? Like with global warming – everyone probably agrees, but what's next? ZK proof as an approach or **theoretical concept sounds great (like "world peace"** or "we support all good and oppose all bad" – everyone agrees, but no one knows exactly what it entails), but who really needs it?

I'm a big proponent of blockchain, but not of using it for everything as the main goal. You often stump blockchain developers with questions like "can the same thing be done without blockchain?" and "is blockchain the optimal technology for this specific problem?" Yes, the **blockchain and crypto community prefers anonymity – and it seems like the ZK proof** problem is (only?) important to the community members themselves: they asked themselves, created a problem, and are solving it themselves. Who else?

Regulators? – they care whether you are in a manhunt or laundering money. Banks, hotels, insurance companies, airlines? – they care that the regulator doesn't hassle them and doesn't make claims about compliance; otherwise, they care more about more customers, simpler onboarding, and higher conversion. Ordinary people as customers? - I'm not sure here: having accounts opened faster, visas processed, and being able to vote online, those might be **the real issues (hypothesis). But "data non-disclosure" – seriously?** Besides people who want to "make a quick buck" on worldcoins issued by Tools for Humanity – who are the real clients for World ID, and what problem does this digital identity and currency solve today?

Technology For Technology's Sake

Looking at ZK-proof (proof without revealing information, as promoted by figures like Altman with Worldcoin and Vitalik Buterin) from a **compliance perspective, it introduces a "rely on" mode**. This mode suggests that if a reputable entity has already verified someone somewhere, others could simply "accept" this verification *without needing to access sensitive personal data*. I may not know everything, and I might be wrong, but this is a discussion I had while establishing a bank, primarily with U.S. regulators, but also with partner banks in the US, UK, and EU. Ok, currently, the **ECB is trialing this concept** with a few banks. The idea is that the second bank may not need to vet the client again or even access their information if another bank has already done so and can simply provide a *yes/no confirmation*.

However, especially **in the U.S. where there's direct opposition**, the prevailing stance is that each institution should be accountable for its own clients and **not pass that responsibility onto others**. Whether or not to accept a client should be your decision, and you should have all the necessary information to make that decision. The end user must provide information about themselves and take responsibility for it. This **approach stems historically from post-9/11 compliance measures**, which aim not just to prevent another such event but to ensure trackability of clients and their funds.

Here lies the crux: if the system relies purely on yes/no tokens in the ledger, it could lead to situations where neither the client nor the bank takes full responsibility, claiming, "It wasn't me; the system automatically approved it, or an error was transmitted about me, but I'm not at fault." This complicates efforts to "follow the money" later on (remember, illicit activities often start with seemingly normal actions by seemingly decent individuals before anomalies occur).

Nevertheless, from my experience—and others may differ—regulators are not opposed to **helping users (or banks) "pre-fill" answers**. However, it's crucial for regulators that users can see what's been pre-filled and have the opportunity to correct it if necessary. They must click "Agree," accepting responsibility for the accuracy of their information during onboarding. Likewise, compliance officers should automatically receive in their data containers the previously answered questions, responses, and even the decisions (as guidance) from previous verifications in the chain.

But, the final approval ("Agree, client approved") must be made by the bank, even if just technically, as the bank must affirm and assume responsibility itself.

Thus, I remain skeptical about Worldcoin & Co—they seem to **neglect understanding (the customer's needs and) the regulatory landscape, focusing instead on technology for technology's sake**. If we rely solely on a set of yes/no hashes at every stage, it will be impossible later to investigate and track transactions and clients effectively. The **concept of yes/no assumes you already know the Truth** (sounds too arrogant, no?), but as I've mentioned, the truth often hinges on the hypothesis. And the hypothesis dictates your risk tolerance (accept the risk vs yes\or).

'Devil's Advocate' Play

It's crucial not only to come up with ideas but also to know when to let them go if it's evident that neither you nor the market is ready. Getting too attached to ideas can be risky. Honestly, I'd approach it from the opposite angle – I'd appreciate it if you could play "Devil's Advocate". Like in science, where you can define an object by what it is or what it is not: let's prove to ourselves that World ID from Worldcoin by Altman is unbeatable, that competing with them is futile because they will always be faster and better. Anyone?

I hope your goal isn't to create a **digital ID just for the sake of it**, but rather to address a specific issue right from the start—even if it's just one small problem. Here are a few problems I see that might be worth tackling:

- Access to (foreign) bank accounts;
- Conducting alternative legal online elections (similar to an online embassy or ambassador, representing a community like change.org but with full KYC);
- Obtaining visas and asylum for forced migrants (though this involves navigating complex bureaucracy).

Consider if there's another use case you could start with that leverages your strengths.

Back to Basics: Re-imagining ATMs for the Digital Identity&Banking Era

How Revolut, AliPay, Binance, and Worldcoin (Could) Lead the Charge in ATM-as-a-Service Innovation

Medium

Dynamic Identity: Why It's a Fluid Concept, Not a Fixed Good\Bad State

KYC is more than just a static 'yes' or 'no'. When it comes to data types you'd want to check, I've outlined some basics here which are generally very important. KYC and ID are a dynamic set of data fields that effectively form a set of variables, the type of questions (the identity type of expected data), the weight of each answer, and the risk tolerance of the receiving side.

Initially, you need an architecture that allows you to ask questions (and save responses) and perform checks (ok, later, as they generate costs). Ideally, you want to **be able to ask more questions or gather more information without having to repeatedly bother end-users.** I understand well how and why you can use compliance and ID to make processes easier and more convenient for everyone. However, regarding blockchain (and Worldcoin in particular) I'm less clear on **how, where (most importantly why) to implement blockchain, at what stages it fits, where it truly adds value**, and where it's just being forced for no good reason.

It's a mistake to try to build another compliance vendor and compete with them or to try to become a 'super-database of all databases' (or a best 'judge' to decide). More useful is a system that allows you to proactively and on-the-go respond to various compliance questions, store those answers, and where necessary, swiftly and easily input them into required processes. But the decision to accept or reject should be made by each service separately (a strict requirement in the USA, while the EU is still deliberating). Technically, the DID is issued by the user themselves, and **you simply assist in its issuance** ('help to pre-fill' vs 'judging yes\no').

As I've mentioned before, regulators don't expect you to know definitively who is good and bad, or to never make mistakes. There is no perfect KYC, no perfect process at onboarding can shield you from fraud and scammers: only about 20% can be caught at registration, the rest are caught during transactions. And to catch them, you need to **set the parameters at onboarding in such a way ("casting a net")** that you can identify anomalies in behavior through quantitative and frequency analysis more quickly and "rewind" effectively when needed.

Compliance didn't start just to prevent tragedies like September 11th, but when such events occur, it's about quickly tracing the involved parties. Remember, **no one is 100% good (ok, only Buterin and Altman, sorry) or 100% bad – everyone performs both good and bad acts**. Real criminals often use layers of good people with legitimate reasons for their transactions – and no system will flag them as bad at onboarding. But it's feasible to set up systems that notice anomalies quicker or trace connections and accomplices more effectively. A new paradigm — using automation and integrations for continuous or **perpetual KYC (pKYC) -** just forget about KYC (or ability to decide yes\no), let anyone who wants a bank account have one, and then use AI/ML to track the bad guys.

The Ribbit Capital's research letter talks a lot here: "A vision of **end user-oriented identification** can take many forms, but often starts with the collection of personal information - perhaps compiling medical records, family documents, or financial credentials in a secure repository. In this world, the infrastructure of identification becomes **reusable** and application-independent; **users decide what, when, and with whom to share**, transferring identification from one application to another and revoking access at their discretion."

They Are Much Better Than Your Chief Compliance Officer

The CIA has announced a new strategy for working with open-source information, aiming to expand and enhance the collection and analysis of data amidst...

linkedin.com

KYC-based Stablecoins

The fund notes here: "The stablecoin market presents an interesting case study; while banking stablecoins, like USDC, are on one hand merely tokens representing dollars in a regulated financial institution, they are also highly innovative, capable of moving around the world 24/7/365, in any amount, in seconds, if not milliseconds. A **tokenized KYC identification document** issued by a sufficiently reliable institution could also possess this same magical ability."

Here I'm keen to explore and test the hypothesis around the evolution of digital identity into a stablecoin concept—an **identity-based stablecoin that embeds KYC and compliance right into the cryptocurrency** itself. Unlike most crypto or stablecoins, which are typically anonymous or lack owner information, we discussed recently with Alex Nikityuk the ability to create our own currency that puts transparency front and center. This currency wouldn't just record transactions; it would also include information about the origin and movement of those transactions (provenance).

In the fund notes: "we see many ways in which data (especially **identity data) is becoming more like money**. The two concepts have always been closely related; money is a ledger of who owns and who owes what, and identity is data about the people, companies, and entities on that ledger. But in a digital age, they are becoming more intertwined – for instance, money is taking the literal form of data (e.g. on blockchains) in the same moment that liquid markets for data are booming, most prominently as AI feedstock. As data becomes more like money, it is becoming more regulated, more important to secure and validate, and more than ever in need of standards to enable interoperability. Given the future we imagine – where people and companies more explicitly value, manage, and exchange data like money – we have started to frame our thinking around the identity space in the language of payments and banking".

Currently, all stablecoins are single- or mono-currency (one for the dollar, one for the euro, etc.), and there are no examples of **multicurrency-stablecoins**. Interestingly, it seems we're not alone in this thought process. (Putin is considering proposing to the BRICS nations the creation of a stablecoin backed by a basket of these countries' currencies. This is partly because Russia is facing challenges with settlements in the national currencies of its trading partners in "friendly" countries. While the Chinese yuan remains fully convertible, similar transactions in Indian rupees are problematic due to the ruble's limited convertibility.)

Today, stablecoins are often more about showcasing technology than solving specific user problems or pains. However, a **stablecoin that doesn't support the local economy in sanctioned totalitarian countries could potentially help local people preserve their savings, safely donate to opposition leaders and projects, and weaken the financial underpinnings of their own local "Putins**."

Ego or a 'Lack of Will' Could Derail These Initiatives

Blockchain and the crypto industry are also very close to realizing the digital identity vision. However, Ribbit Capital notes that success here may be hindered by too much focus on technology (as it is only one of the components and variables) and fragmentation (the inability to agree on a common standard). Meanwhile, blockchain and crypto startups may find themselves in competition rather than collaboration.

In general, the Ribbit Capital's research letter talks a lot about how EGO (often referred to in the text as "lack of will") can be one of the stop-factors in the development and success of digital identity initiatives: both political leaders may ultimately fail to agree on uniform standards (as the world does not need a multitude of national digital identities), and fintech founders, digital banks, **blockchain, and crypto startups might compete against each other instead of collaborating.** As a counterexample of the ability to collaborate and collectively profit, the authors cite the creation of payment systems like VISA. (The authors compare the architecture of card systems to the possible future network of digital identity - issuer, acquirer, holder.)

Worldcoin could become a Biometrics-as-a-Service with its...

Imagine Worldcoin rolling out as the go-to for Biometrics-as-a-Service, complete with its very own biometric ATM-station. Imagine unboxing...

Medium

Retina-without-KYC

Is anyone familiar with how this actually functions or who successfully implements it? To refresh your memory, in December, developers rolled out World ID 2.0, now integrated with various platforms including Telegram. Tiago Sada noted that the protocol has been expanded to include Shopify, Mercado Libre, Reddit, Telegram, and Microsoft's Minecraft among others. These integrations could potentially enable some users to use their World ID to log into these services.

From what I gather, all that's added is a bot in Telegram or Discord that verifies a World ID—not for registration/login but merely for verifying an existing user on the platform. Doesn't that seem somewhat futile? I was expecting something like a "Sign up with World ID" button on Telegram or Discord! Isn't this just a typical "integration" that involves big names but lacks depth in what actual integration means? Perhaps it's mostly marketing hype.

Moreover, Worldcoin doesn't operate with sanctioned countries and largely serves as a method of authorization rather than a full digital identity. Is it possible that investors and other "experts" in the market are too herd-like, afraid to challenge Altman? When he claims "Worldcoin does everything and solves all problems," they fail to scrutinize and instead recommend others to "build on their already prepared rails."

Solana, like other platforms, has its pros and cons; you can develop similar solutions on it. However, this doesn't eliminate several issues: 1. Technical risks (consider how often their blockchain has faced disruptions); 2. "Understandability" for institutional users (Stellar is already functioning for Moneygram, but is Solana only significant for meme coins so far?).

I'm not entirely sure about the benefits or drawbacks of the TON blockchain (and generally, I prefer to focus on the user and their needs rather than the technology itself), but regarding Telegram, it might be more convenient for some users to respond to onboarding queries in the format of Telegram chats. This hasn't been tested yet, but it's an intriguing approach. Additionally, it could serve well as an RFI-messenger (request for information), where various bank employees discuss a client or their transaction, need to query the user further, and then forward the responses and their insights to another partner bank or correspondent bank.

Why doesn't Nothing release its own crypto-phone or collaboratio...

How cool would it be if Nothing dropped a crypto-phone or teamed up with Revolut or Worldcoin, right? How awesome would it be to see (those...

linkedin.com

I may not be a blockchain guru, sorry in advance!

But my experience in digital banking, compliance, and navigating the intricacies of global financial regulations has given me a pretty solid footing. Over the years, I've launched and invested in multiple digital banks across various countries, including my own ArivalBank.com. I've plunged into the compliance sector, backing three startups and personally securing a banking license in the USA and a securities license in Singapore. My operations stretch across 28 countries, making me all too familiar with the regulatory dances in the USA, UK, and EU—everything from financial oversight to the gnarly issues of data storage and processing.

However, regulatory bodies prefer a **precedent-based approach** to compliance and KYC, always asking whether a reliable entity has previously vouched for an identity. Working closely with partner and correspondent banks has deepened my understanding of KYCC, ID reusability, and the "rely on" compliance mode across different regions. This hands-on approach has shaped my view on the emerging needs for digital identity verification—specifically, why blockchain could be a game changer in the realm of decentralized identity (DID).

Currently, the blockchain space is awash with **speculation and trading, yet tangible applications that solve real-world problems are scant. I advocate for a ground-up strategy that starts with real people facing real issues** who are willing to pay for real solutions. Turning to the broader blockchain landscape, Forbes has highlighted a significant issue: many major blockchains, classified as "crypto zombies," reportedly lack functional value and are primarily geared towards speculative trading of digital assets. Among these, networks such as Ripple (has announced plans to launch a US dollar stablecoin later this year, aiming to compete directly with established players like USDT and USDC, potentially shaking up the stablecoin market), Ethereum Classic, Litecoin, Algorand, and Cardano have been cited as lacking tangible benefits. Despite their market valuations exceeding $1 billion and a collective worth of over $116 billion, **activities on these platforms remain minimal. The industry faces criticism for its focus on hyperbolic claims rather than delivering real-world applications**, resembling early-stage companies or venture capital funds that have amassed excessive funds without clear plans for utilization (this scenario underscores a broader challenge within the crypto sphere: a lack of accountability to users).

High-Risk Compliance for BaaS and Correspondent Banks

Starting from January 1st, FinCEN introduced a new regulation, AMLA, which requires banks to conduct KYCC, which affects correspondent and BaaS banks...

linkedin.com

Blockchain as a language (and compliance as a language too)

Blockchain could well be the language (or as my friend Andy Done told - "operational system or like Linus") we need for compliance—a dynamic, adaptable framework that respects the nuances of identity data without compromising privacy. But this isn't just about reducing the need for sharing personal information like names or emails to access services; it's about creating a **reusable identity** that can streamline user interactions without sacrificing security or compliance.

Cryptocurrencies initially promised anonymity but evolved under the pressure of regulatory compliance. This shift isn't necessarily a setback but a feature that could lead to the development of **compliance-first financial solutions, mirroring India's Aadhaar** system in form and function. The challenge now is to orchestrate and hash multiple layers of a person's or company's data across jurisdictions into a coherent, accessible format—this is where real value lies.

The broader issue of power centralization and accountability in such a decentralized network remains a hot topic. **How do we safeguard against the malicious alteration of data by any node within the network?** My several short discussions with the Worldcoin team, Vitalik Buterin and his zuzalu-mates in Istanbul, revolving around digital identity, have highlighted the nebulous nature of the demand for these advanced blockchain identities and the real problems they aim to fix. The main question every day was - aside from technical advancements in blockchain, it's unclear who specifically needs this identity and what real problem it solves. Moving forward, my focus will be to refine and implement these digital ID solutions (first focus on 're-usable' and pre-filling) among digital banks first, prioritizing a system that not only preserves but enhances user identity through practical, real-world application. Maybe I am wrong here.

Thanks for sharing your thoughts in advance —it really spices up the discussion and brings a variety of perspectives!

How could World ID be better? Or at least useful

World ID from Worldcoin and Tools for Humanity is currently an absolutely useless thing - no one can answer the simple question of who specifically need...

linkedin.com

Comments