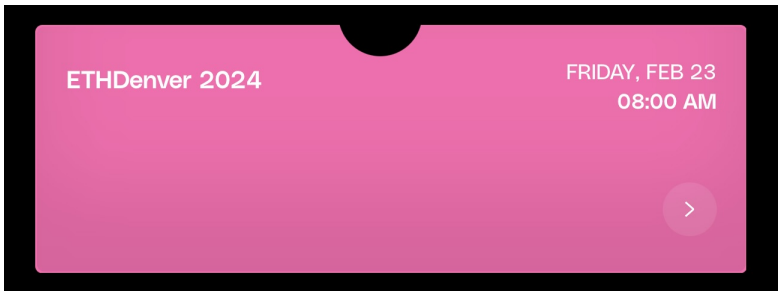
Fully onchain ticketing with ZK proofs

This year, I got to Denver for the ETHDenver community conference a few days before the main event. Mainly because we were not in a rush like we were a year ago, and secondly because the last two days of conference weren't as productive as the first two, and we missed many pre-conference meet-ups and side events.

So today, the day after arriving, I got to the *Spork Castle* to get my ticket. I don't even remember how I got the ticket on my phone anymore, because I applied in the very early days of ticket application - but I do remember going through several steps to ensure my ticket receipt was in the Tokenproof app.



Up until today, I honestly thought there was no reason for me to through connecting a wallet, signing some off-chain signature, clicking on some links, scanning a QR code or whatever just to have a banner saying I have a ticket for a conference. Why couldn't I just use Eventbrite, Lu.ma or other event platforms?

I mean, I work in crypto - I believe that eventually, everything will be onchain. But I also hope it will be *easier* to save things onchain than on a centralised server (eventually). And that was **not** easy. Lu.ma is easy. You just write your email, answer some custom questions the organiser prepared, and you're in - or waiting for approval.

But we know that Lu.ma is used for 'simple' events: a meetup, a side event, a cocktail night, etc. For bigger events like the ETHDenver Main Event, and in general for high-attendance events that need to comply with local regulations, you need to identify who's attending.

And you do that by asking for a passport or an ID along with the original ticket receipt / QR code at reception.

Well, today, as I went to get my ticket, I even stopped by the hotel to take the passport (I usually only bring my ID with me) bc I was not sure I could get the ticket with just my ID. Then, I discovered I didn't need any identification at all.

Now, I don't know if this was on purpose, or because I got the ticket before the event /for whatever reason), but even if that was a mistake, and I should have gotten my ID / passport checked, it got me thinking that *onchain* solves the identification dilemma for events and any activity that involves creating a list of people involved in doing something:

> *"How can event organizers safely check-in participants without knowing their identity?"*

Well, it turns out, with blockchain they can.

Let's say I want to go to an event that offers a fully onchain ticketing system in an off-chain world . To buy a ticket, I would need to go through these steps:

steps:

1. Go to the event page and click a button to get the ticket
2. Sign-in with my wallet
3. Go to a self-attestation page to put my personal info (Name, Surname, Address, Phone Number, ID number, etc.)
4. Sign an onchain transaction to attest to my personal information, and zk-proving that
    1. If I have a personal attestation already, I can just sign with that existing one and include that in the ticket payment transaction
5. Pay what I owe and get my ticket in an app like Tokenproof
6. At the event's reception, just show the ticket's QR code

In this user experience, the ID check is not required because two major assumptions are made:

- The phone you're showing the QR code with is yours and only you know how to access it
- ID checks at reception are only made to check if the photo on the ID matches the face of the person it's being handed from, and that the name on the document is the same on the ticket - no other check is being done, like checking the **integrity** of the document, i.e. if it's a real document or a fake one.

This approach works really well for any kind of event, because those trust assumptions are already made in the current world.

I want to emphasise that, with this approach, **identity is implied in the ticket**.

So basically, in the same way, identity can be implied (enshrined) in any process that doesn't require an integrity check of the ID.

I'm not saying that it's not possible to do the same for processes that require an integrity check - just that it's a different story. To solve the identity integrity problem, we would need to tackle the whole identity issuance aspect. And it's a much bigger and harder problem.

Date: 2024-02-27
Words: 772
Time to read: 3 mins

Newer Older

8th March 2024
About L3s and the Superchain, ...

15th February 2024
The Importance of Atomic Deve...

Tags Archive RSS feed Twitter Instagram GitHub Email QR Code