The Whiteboard

Reclaiming Our Privacy with Zero-Knowledge Proofs

Kit Colbert
October 27, 2022

A little over a month ago, I published a blog about the future of the Internet – what people are referring to as Web 3.0. I explained that while this generation of the Internet has been characterized by third-party aggregation of user-generated content (such as social media), Web 3.0 would be characterized by privacy, where users regain control of their own information.

Today, I wanted to explain a bit more about "zero-knowledge proofs" (ZK Proofs), the technology that will make this a viable reality. While the technology behind it is complex, the concept of ZK Proof is quite simple: it's a method where one party can answer a question without directly providing an answer (e.g. the date) but instead by going through a verification process. Because of its potential utility, ZK Proofs will continue to gain traction in the immediate future, not just in the context of Web 3.0, but for other use cases, as well, including cryptocurrency (allowing verification of transactions without exposing the sellers' and buyers' identities), distributed ledger technology, online voting (counting votes without revealing voter identity), and more. Basically, any situation requiring privacy and security to verify credentials or data can benefit from this technology.

Why is this technology important?

In an age where personally identifiable information (PII) can be used to unlock so many doors (for example, a social security number can be used to steal a person's identity, allowing a hacker to empty the victim's bank account, open credit cards, and more), privacy has become critically important. In other settings, companies may wish to share data (for example, to build better machine-learning models) without exposing intellectual property.

It is important to note that ZK Proofs are not perfect — they're probabilistic. ZK Proofs are also computationally intensive, relying on complicated algorithms and multiple interactions between the parties involved. This can add latency to transactions (making it challenging to implement in applications that depend on speed). There are other problems, as well, such as the fact that if a party (such as the holder of cryptocurrency) loses the keys to their information, there's no way to recover the data.

How it works

It sounds a bit paradoxical: how can you transmit information to someone without exposing the information itself?

First described in a 1985 MIT paper, authors Shafi Goldwasser and Silvio Micali demonstrated that theorems contain more knowledge than just the fact that they are true or false. To translate this into a real-world situation, let's use the example I described in my Web 3.0 blog, where someone is applying for a mortgage. The mortgage bank needs to know that 1) the applicant makes enough money to make the payments, 2) the applicant has a stable job, and 3) that the applicant's debt-to-income ratio is not so high that they cannot comfortably afford the payments. However, the data the applicant provides to the bank also includes extra information — the name of the person's employer, the applicant's preci

person's employer, creditors, social security number, and more. With ZK Proofs, banks could verify that the applicant's income is adequate, that they have a stable job, and that they have a reasonable debt-to-income ratio without needing to know all of the details of these factors.

ZK Proofs research at VMware

VMware is investing in substantial research in this area. In the paper "UTT: Decentralized Ecash with Accountable Privacy," published in April this year, VMware authors discuss their work on UnTraceable Transactions (UTT). UTT is the first ecash system to provide decentralized trust by implementing the ledger, bank, auditor, and registration authorities via threshold cryptography and Byzantine fault-tolerant infrastructure. UTT will balance accountability and privacy by implementing "anonymity budgets," which means that users can anonymously send payments but only up to a limited amount of currency per month (reducing the likelihood that these systems will be used with criminal intent). UTT is also tailored for high throughput and low latency, making it more practical for applications where performance is critical. You can read more about this work (and even try a demo of UTT on your laptop if you have the technical chops) in this technology preview.

I look forward to hearing your thoughts about the applications and viability of ZK Proofs in the comments.

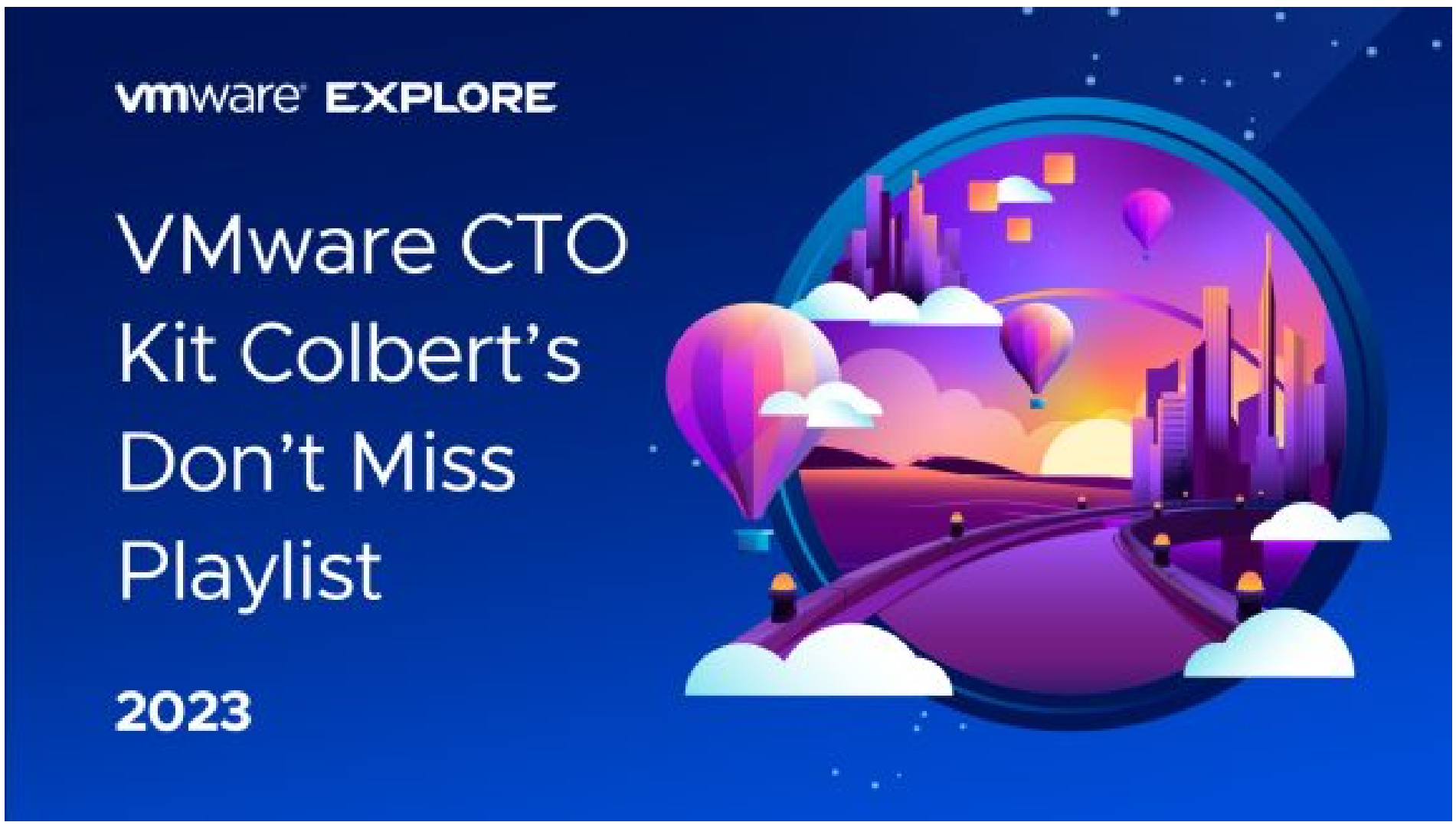
Best,

Kit

Kit Colbert

Kit Colbert is VMware's Chief Technology Officer, driving technical strategy, innovation, evangelism, and SaaS transformation across VMware's engineering organization. Previously, he was VMware Cloud CTO, GM of Cloud-Native Apps, CTO...

Related Articles



VMware Explore 2023

Kit Colbert's Don't Miss Playlist 2023

Kit Colbert

August 18, 2023

The Whiteboard

Why a Supercloud Architecture is the Ticket to the Next Level

Kit Colbert
March 14, 2023

The Whiteboard

The Multi-Cloud Journey: Skipping Over the Chaos to Arrive at “Cloud Smart”

Kit Colbert

February 15, 2023

The Whiteboard

Where Introspection Meets Action: A Path Toward Better Allyship

Kit Colbert
February 8, 2023

The Whiteboard

Where Tech is Headed in 2023

Kit Colbert

January 24, 2023

Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Name*

Email*

Website

Save my name, email, and website in this browser for the next time I comment

POST COMMENT

vmware by Broadcom

Company

About Us

Executive Leadership

News & Stories

Investor Relations

Customer Stories

Diversity, Equity & Inclusion

Environment, Social & Governance

AI at VMware

Careers

Blogs

Communities

Acquisitions

Office Locations

VMware Cloud Trust Center

COVID-19 Resources

Support

VMware Customer Connect

Support Policies

Product Documentation

Compatibility Guide

Terms & Conditions

California Transparency Act Statement

Hands-on Labs & Trials

Twitter

YouTube

Facebook

LinkedIn

Contact Sales

Terms of Use

Your California Privacy Rights

Privacy

Accessibility

Trademarks

Glossary

Help

Feedback