# Crypto 3.0 Will Be More Human: Causes for Optimism in Tumultuous Times


By Jason P. Davis , INSEAD

**At a recent INSEAD event, Ethereum co-founder Vitalik Buterin revealed technologies to manage online identities, preserve privacy and ensure the responsible use of AI.**

Despite the current crypto winter and general uncertainty surrounding the sector, **blockchain technology** still attracts plenty of interest in its capabilities – be it facilitating a more decentralised financial system or powering Web3 applications.

At a **Tech Talk X** organised by Ethereum Singapore and **INSEAD's Savvy Salamander Study Club**, I introduced Ethereum co-founder Vitalik Buterin to a full house at INSEAD's Asia Campus. Besides touching on recent developments in the Ethereum ecosystem – such as the long-awaited network switch from proof-of-work to proof-of-stake – he unpacked tools that

can help us tackle some of the most pressing problems in today's digital space, such as identity and trust issues, privacy concerns and the **ethical deployment of AI**.

## The evolution of crypto

Crypto is moving into a third stage in its evolution, which I dub Crypto 3.0. In its initial form, Crypto 1.0 was focused on conducting simple peer-to-peer transactions over a distributed ledger in the Bitcoin blockchain. In Crypto 2.0, we saw the explosion of decentralised applications including DeFi and NFTs through smart contract blockchains such as Ethereum, which created a bona fide decentralised computer usable by anyone. Crypto 3.0 will build on these innovations and equip people with the tools to control their identities on crypto networks, making it much more user-friendly and easier to address prevailing privacy concerns.

Under the mechanisms set out in the first two stages, crypto wallets and transactions are still fully public and transparent, despite being anonymous. This is usually considered a good thing, as it allows participants to be fully aware of counterparties' balances and perform risk-mitigation activities, or for authorities to trace criminal activity conducted over the blockchain. Ironically, both of these features were lacking in the most recent blow-ups of **crypto hedge funds**, **centralised exchanges** and **quantitative trading firms** that have been consuming the news.

However, there are many valid reasons why regular users would want greater privacy when using these networks, including better protection from hackers or an intrusive government, or to keep identities secure. Crypto 3.0 really speaks to the broader idea of identity on the internet, and how much control we have over it.

Technologies have already been created to address this problem. Ethereum Name Service (ENS), for example, allows people to generate human-friendly and readable usernames on the Ethereum blockchain that they can use to conduct secure decentralised transactions. Another crucial development that will play a major role in the coming years is expanding the use and applications of zero-knowledge proofs.

## Unlocking zero-knowledge proofs

Buterin addressed the **growing importance of zk-SNARKs**, or “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge”. Put simply, these are a form of cryptographic proof that allows a user, creator or owner to confirm the validity of certain data without revealing everything about the data itself. It enables individuals to be selective about what they reveal and when they reveal it (while proving its validity), even to the extreme level of having “zero knowledge” of what is inside the data stream. This differs from the current predominant system of transacting over maximally transparent blockchains.

Besides its **scalability applications**, zk-SNARKs have huge privacy ramifications. By allowing people to only reveal certain aspects of the data in question, they can establish validity while attaining greater control over their privacy. For instance, zk-SNARKs can be used to prove that you made a specific crypto transaction without revealing your identity, pointing back to your wallet or disclosing information about other transactions made from that wallet.

There are plenty of privacy applications for this technology, particularly when you want to achieve cryptographic-level assurance without revealing lots of data. These range from smart contracts and voting systems to account moderation and reputation protection. Furthermore, it can be used to prove that you are a unique human, a member of a particular community or trusted by other accounts.

Another key application of zk-SNARKs is in remixing services, where users can send in their coins – which are mixed with coins from other sources – and withdraw random coins in return. These are accessed by people who want to achieve greater privacy and anonymity when using a public wallet, as the mixing of coins makes it virtually impossible to trace them back to their original source.

However, remixing services are facing greater scrutiny and regulation due to their potential connection with criminal activity. The United States government recently **imposed harsh sanctions on Tornado Cash** for its alleged laundering of virtual currency. As a result, many exchanges such as Coinbase and Binance have been hesitant to go anywhere near remixing services.

But with zk-SNARKs, users could provide specific information that proves they’re not using the platform to carry out illegal affairs, without disclosing

anything that would reveal their identity. This could limit the ability of hackers and fraudsters to benefit from these services, which would make them safer and help alleviate the concerns of exchanges and regulators.

**How’d you solve a problem like AI?**

On the flip side, there are instances when we want to prove our identities or the “humanness” of things on the internet. Given the launch of generative AI models that rely on Large Language Models (LLMs) such as GPT-3, DALL-E and stable diffusion, we’re seeing a huge increase in the amount of realistic AI content that could easily pass off as being created by a human. The probability that we’ll soon be flooded with such content is a real concern in the AI community, and many are hoping that crypto can help solve the problem.

In response to **my question about the problem of generative AI**, Buterin noted that it used to be relatively easy to identify deepfakes, bots and AI-generated content. But it will become increasingly difficult to discern this as the content becomes more sophisticated. The consequences could include spending our time interacting with bots that we think are real people, or the proliferation of more believable deepfakes that can be used for malicious purposes. We may also begin placing more of a premium on human-generated content. However, if almost all the content on the internet is produced by AI, we could simply be unable to find these human-generated works.

Buterin suggested using a cryptographic version of digital signatures (which are used to identify websites) or zk-SNARKs to confirm human identities or tag content as being produced by humans. Indeed, zk-SNARKs would allow for human-generated content to be labelled as such without revealing which human produced it, thereby preserving privacy. He added that the timestamping feature of blockchains could help differentiate original content from reproductions or fakes.

**Towards a more decentralised future**

Many people have the perception that crypto is purely about decentralised finance and anonymous transactions – in short, all about the financial applications and less about the human side. But Crypto 3.0 looks to be a world where we will have access to tools that are much more focused on the social elements of the internet.

As the landscape evolves and we see greater efficiency, innovation and adoption, I believe there will be even more ways for us to establish and manage our digital identity, build reputation and ensure privacy, while protecting ourselves against bad actors. This could eventually lead to the creation of a decentralised social network and social media with new capabilities to facilitate this.

The evolution of the crypto space into one that's more focused on the human aspect could have huge – and hopefully positive – repercussions for all internet users, and is certainly something to keep an eye on.

**Find article at**
https://knowledge.insead.edu/entrepreneurship/crypto-30-will-be-more-human-causes-optimism-tumultuous-times

---

## About the author(s)

**Jason P. Davis** is an Associate Professor of Entrepreneurship and Family Enterprise at INSEAD. He studies digital transformation and innovation in large enterprises, especially Big Tech companies in Asia and the US, as well as the strategies of start-ups in digital platform ecosystems, such as the iPhone and Android mobile ecosystems.