

David Chaum Announcing XX Network & Nym Partnership at Ethereum Cypherpunk Congress 2, Buenos Aires

Sun, Nov 16, 2025

SPEAKERS:

David Chaum

David Chaum 00:10

With AI on the rise, what does the future hold for us? Well, actually, I'm thrilled to be able to share my thoughts on this with you, but I'd really rather be there in person. In any case, we've made a lot of progress over the decades raising awareness of the privacy issue. Not many people knew much about it when we started, but now much of the public is very concerned about privacy and realise how crucial it is.

David Chaum 00:46

Still, most people aren't willing to go way out of their way to protect their own privacy, because the tools aren't ideal. There are some people who will take the extra effort, but and then there's us who are trying our utmost to bring this issue to the fore and make the world a better place.

David Chaum 01:12

Stepping way back, we are at what I would like to call the Chaumian triple point. In thermodynamics, there are three common phases of matter: solid, liquid and gas, and only at the triple point can even two, let alone three, coexist. As in thermodynamics, once temperature or pressure deviate, the triple point must resolve decisively in one phase or another.

David Chaum 01:46

Throughout almost all of human history, what information technology breakthroughs there may have been were not automated. This is what we might call, by analogy, the gas phase, some of it's still with us: witness the whiteboard or pencil and paper.

David Chaum 02:07

Today, automated information technology is advancing exponentially. The powers that be seem hell bent on this. It corresponds, in our analogy to a rise in pressure. The triple point we are at is actually tiny relative to the length of human history, but this is the kind of chaotic interval when things can easily be tipped one way or another, hugely empowering the few doing the tipping.

David Chaum 02:45

For the triple point as pressure rises, analogous again, to more IT automation and advancing AI, one direction is the frozen phase where information technology is used to control us, whether by the elites or by AI itself. Frozen is when all that is human is frozen out of people. Picture a frozen landscape of a

formerly inhabited planet, but there's a third phase. While you think of what this third phase might be like for us, for the benefit of those who are new here, let me give a brief history of my own efforts.

David Chaum 03:37

It started with an epiphany in the late 1970s that privacy would be crucial to preserving human freedom in the information age, I devised and published a technique to allow untraceable communication, a key technology called mixing that we'll come back to in a few minutes. Then in the early 1980s the National Security Agency was trying to declare cryptography to be born classified like nuclear bomb making, and threaten jail for even holding a conference on it. So being a grad student at Berkeley, I decided it was essential to organise an international conference on cryptography, risking spending my life in jail to set cryptography free, because I realised how crucial it was.

David Chaum 04:32

At that conference, I introduced e-cash, the first digital currency. Its privacy was what today you could call quantum secure - privacy not even a powerful quantum computer could break because breaking it is mathematically and physically impossible. Later, I published in Scientific American how to protect not only money, but messaging and all manner of personal information. It also with quantum secure privacy. All the data that organisations or governments have about you could be protected against quantum attacks with keys that are held by you, a paradigm shift that inspired many.

David Chaum 05:18

Then I generalised this to multi-party computation with quantum protected secrets, which won a theoretical computer science award 30 years later. It showed essentially that if you can define an information security solution, it can be built securely. That's crucial to what I'm about to propose.

David Chaum 05:38

Back to the triple point that we find ourselves at today, we have automated our information technology with computers, the internet and now artificial intelligence. This has given us access to information around the globe and the ability to communicate near instantaneously with other people anywhere. But it's also engendered mass enterprises that manipulate information and that surveil and even manipulate us. We've seen intrusions on freedom, liberty and even human life through all this surveillance and manipulation, we as a population have failed to control information technology. Elites control it, ordinary people do not. Arguably, much has been sucked out of civilization by AI already.

David Chaum 06:33

So in our analogy, what's the alternative to the frozen phase? It is liquid, a symbiosis. Picture dolphins frolicking in clear water, human potential unleashed by what Richard Brautigan, I think probably inspired by Richard Feynman when both at Cal Tech called "Machines of loving grace". In this liquid phase state, AI helps us run things and improve the world, but AI does not dominate us. We work together with AI to elevate human potential.

David Chaum 07:21

I have specific proposals for how to achieve this - new kinds of AI assisted sample voting and systems to address the multi polar world with its AIs, and even a somewhat related way to solve global warming. Let me invite you to reach out if you'd like to help me advance these ideas. Please have a look also at my website, chaum.com, that's my last name.com, thanks.

David Chaum 07:53

Society is now at a critical juncture. We could transition to the frozen state or to the liquid state. Advancing AI is the exponential rise in pressure driving the irreversible choice, and we will certainly go one way or the other and not both. One path will dominate and erase the other, and society will undergo a phase transition out of the triple point. This group assembled here, look to your right and look to your left. We have real power to influence the direction. The chaos of major civilizational change often means small forces can tip things towards specific outcomes.

David Chaum 08:45

This brings us to the present moment. We need something very fundamental at a human level right now, a way for people to participate in social movements without fear of retribution. That fear, that threat strikes at the heart of our freedom. People must be able to find information and communicate with others, without governments or anyone else being able to observe them. Mass surveillance has led to later persecution, as has happened in countries where even entire activist movements were wiped out.

David Chaum 09:26

The answer is mixing, which I would like to now return to. Mix networks send messages concealed in multiple layers of encryption through a series of independent network nodes. Messages are unwrapped partially along the way, and finally at the destination node where they're completely decrypted. It's the foundation of the truly private communication system we need.

David Chaum 09:57

So I've been asked to announce here that the two mix-network based privacy systems, xx network, which I founded, and Nym, have formed a partnership to provide a VPN accessed decentralised messaging system that addresses just this issue, frankly, it will be far and away the best privacy for participation that the world has ever seen. We have the technical capability today, if we pull together, we can provide the platform and the vision to help society choose the right direction. We are the ones who can do this, and the time is now.