INTERVIEW DAVID CHAUM: "BLOCKCHAIN WILL DECENTRALIZE POWER"

David Chaum

Publication date: 18-11-2019

David Chaum (1955) is one of the most important pioneers in encryption. His research laid the technological basis for blockchain and bitcoin. On 21 November 2019, Chaum will be awarded the Dijkstra Fellowship by CWI.

He is called the 'Godfather of Cryptocurrency'. In 1990, when the general public had never heard of the Internet, David Chaum founded DigiCash: a company that could provide financial institutions with a system for secure and anonymous digital micro payments. It was no coincidence that DigiCash's head office was in the Matrix building at the Amsterdam Science Park. Chaum had been with the Dutch National Research Institute for Mathematics and Computer Science (CWI) since the second half of the 1980s as head of the cryptography department. In 1982 he had written a groundbreaking dissertation on how a blockchain-like technology could be developed to enable digital transactions without the need for an authority – such as a bank or credit card company. After he founded the International Association for Cryptologic Research in the same year, his star had risen rapidly. By the time he arrived in Amsterdam, he was considered by peers to be one of the very best cryptography experts in the world.

How do you feel about the fact that CWI is honouring you with the Dijkstra Fellowship Award?

"Any time I return to CWI, it feels like a homecoming: so much of my work began here, and the inspiration I received and the enthusiasm I found at CWI often had me happily working late into the night. So I'm hugely honored and deeply humbled to be one of the inaugural Dijkstra Fellows."

What brought you into the field of encryption?

"Encryption has always fascinated me for two reasons. On the one hand, it's theoretically fascinating. The complexities of codes, signatures, and verification are endlessly rewarding for a curious mind. But encryption is also of fundamental importance to our day-to-day lives, whether or not we realize this. Proper application of encryption can make communications secure, commerce reliable, and voting trustworthy. I firmly believe that it can make this world a better place."

How was CWI instrumental or inspirational to your work on encryption?

"CWI brought me into close proximity with some of the world's best thinkers on privacy, encryption, networks, and the Internet. The conversations about digital identity and virtual sovereignty the mainstream is finally addressing first happened at CWI twenty, thirty, or even forty years ago."

You are the founding father of digital cash. What brought you to that idea in the first place?

"New ways of communication and connection often necessitate new ways of understanding money. A few hundred years ago, paper cash was an innovation, necessary because you didn't want to lug your hoard of gold everywhere. Similarly

ago, paper cash was an innovation, necessary because you didn't want to lug your hoard of gold everywhere. Similarly, once you have banks and branches and networks, you'll get checks, and eventually credit cards. It seemed obvious to me that the Internet, which empowers people everywhere to connect and communicate with each other, would need its own currency."

Do you sometimes think you were too far ahead of the times with that idea?

"I wasn't that far ahead of the times: I'm still around to see the times come around! I think of Charles Babbage, who invented, but could not build, an 'Analytical Engine' computer in the mid-nineteenth century. In all seriousness, it has been a pleasure to see the explosion of digital currency over the past decade."

Is blockchain heading in the right direction with Bitcoin? Or do you think the current state of the technology is hindering mass introduction?

"I'm not sure blockchain is headed in a single direction. Every day it seems that new approaches and new technologies are being introduced. The growth of blockchain has outstripped the growth of Bitcoin. That said, it's undeniable that Bitcoin's limitations, particularly calculation speed and energy expenditure, sometimes affect observers' perspectives on blockchain as a whole."

Can a digital currency of limited supply, like Bitcoin, ever play a significant role in the economy?

"Bitcoin has launched a worldwide movement and attracted millions of people to the promise and importance of digital currency. That's a wonderful achievement. I find it exciting that in my global travels, I'm constantly meeting people animated by the concerns I first raised many years ago about the importance of digital privacy and security."

What is you viewpoint on Facebook's Libra?

"To the extent that Facebook and their partners are focused on building Libra, they are paying a compliment to the blockchain community. When some of the world's largest and most powerful companies are following your lead, you must be doing something right. With that said, I believe strongly that the digital citizens of the world want a decentralized network open to all, rather than place their trust in big corporations with a mixed record on user privacy."

Are you currently working on new breakthrough cryptography protocols?

"Praxxis, our forthcoming high performance digital currency and blockchain technology, will introduce quantum-resistant vertical and horizontal privacy. It will be possible to, for example, send a payment in such a fashion that outside eyes — and I include my own eyes as outside eyes — will be unable to identify either sender or recipient."

Do you think that it's already possible to lay the groundwork for cryptography protocols which are quantum computer proof?

"Blockchain has a unique ability to decentralize power, and it's essential that we not cede 'quantum supremacy' to Google or whoever else has the fastest computer. We're already at work on building a quantum-resistant protocol. Will it grow and evolve and change? Of course it will, but the groundwork is already there."

By: Ed Croonenberg

Related content

-  David Chaum and Guido van Rossum awarded Dijkstra Fellowship Centrum Wiskunde & Informatica (CWI) will grant the honorary title 'Dijkstra Fellow' for the first time in its history. This edition the Dijkstra Fellowship will be awarded to David Chaum and Guido van Rossum.

- 2021
- 2020
- 2019
- 2018
- 2017
- 2016
- 2015
- 2014

EVENTS

- PHD DEFENSE YOUS VAN HALDER (SCIENTIFIC COMPUTING)
- PHD DEFENCE FARROKH LABIB (A&C)
- DUTCH SEMINAR ON OPTIMIZATION (ONLINE SERIES) WITH ANDREAS WIESE (VU AMSTERDAM)

MORE...

INFO

Centrum Wiskunde & Informatica (CWI) is the national research institute for mathematics and computer science in the Netherlands. CWI is part of NWO-I, the Institutes Organisation of NWO.

ADDRESS

CWI Location:	Science Park 123 1098 XG Amsterdam NETHERLANDS
Postal address:	P.O. Box 94079 1090 GB Amsterdam NETHERLANDS
Phone:	+31 20 592 9333

E-mail: INFO@CWI.NL

CONTACT

DISCLAIMER