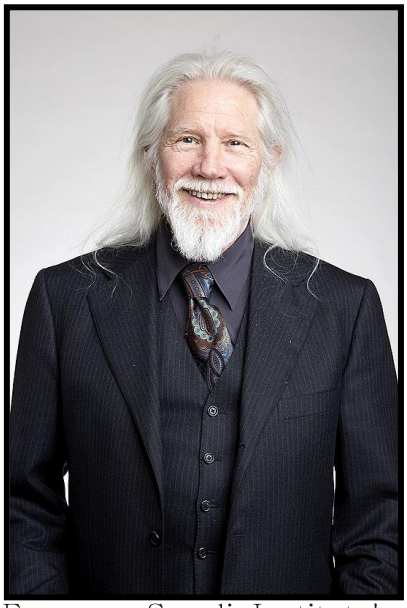
Eurasia Blockchain Summit

Whitfield Diffie



(born June 5, 1944), ForMemRS, is an American cryptographer and one of the pioneers of public–key cryptography along with Martin Hellman and Ralph Merkle. Diffie and Hellman's 1976 paper New Directions in Cryptography[5] introduced a radically new method of distributing cryptographic keys, that helped solve key distribution—a fundamental problem in cryptography. Their technique became known as Diffie–Hellman key exchange. The article stimulated the almost immediate public development of a new class of encryption algorithms, the asymmetric key algorithms. After a long career at Sun Microsystems, where he became a Sun Fellow, Diffie served for two and a half years as Vice President for Information Security and Cryptography at the Internet Corporation for Assigned Names and Numbers (2010–2012). He has also served as a visiting scholar (2009–2010) and affiliate (2010–2012) at the Freeman Spogli Institute's Center for International Security and Cooperation at Stanford University, where he is currently a consulting scholar. Diffie was born in Washington, D.C., the son of Justine Louise (Whitfield), a writer and scholar, and Bailey Wallys Diffie, who taught Iberian history and culture at City College of New York.[8] His interest in cryptography began at "age 10 when his father, a professor, brought home the entire crypto shelf of the City College Library in New York." At Jamaica High School in Queens, New York, Diffie "performed competently" but "never did apply himself to the degree his father hoped." Although he graduated with a local diploma, he did not take the statewide Regents examinations that would have awarded him an academic diploma because he had previously secured admission to Massachusetts Institute of Technology on the basis of "stratospheric scores on standardized tests."] While he received a B.S. in mathematics from the institution in 1965, he remained unengaged and seriously considered transferring to the University of California, Berkeley (which he perceived as a more hospitable academic environment) during the first two years of his undergraduate studies. At MIT, he began to program computers (in an effort to cultivate a practical skill set) while continuing to perceive the devices "as very low class... I thought of myself as a pure mathematician and was very interested in partial differential equations and topology and things like that."