Paolo Bondi

David Chaum has made incredible contributions to the advancement of cryptographic research. Born in 1955, Chaum was given his doctorate from the University of California, Berkeley in 1982. In the same year, he also founded the International Association for Cryptographic Research. The IACR is a non-profit association with its main purpose to further research in the Cryptographic field. They hold three conferences and four workshops that bring in computer scientists and cryptographers from all over the world. Soon after founding IACR, Chaum furthered him passion in education by teaching at NYU and UCSB for five years before going on to form a cryptography research group called the National Research Institute for Mathematics and Computer Science (CWI) in Amsterdam.

The more notable research contributions that put Chaum on the Crypto-map are his contributions to the Digicash corporation. Chaum pioneered the development of blind signatures, which is a form of a digital signature that allows the content of the message to be disguised before it is signed. Ensuring the message is disguised is an essential element in anonymous communications, especially when the contents of the message possess monetary value. Furthermore, Chaum is also responsible for the invention of a undeniable signature, which allows the signatory to limit who can verify the signature. This signature process utilizes a verification process that is interactive, so that the person signing the message does not have access to its contents. In 1991, Chaum also created a for of signature called the group signature. This allowed a message to be signed by an entire group of people. The responsibilities within the group will be delegated by a group leader, and can revoke the anonymity of an individual signer. Due to his findings in his 1982 paper, as well as his advancement in digital signatures, Chaum is recognised as the inventor of secure digital cash.

While Chaum has made notable advancements in the field of digital cash, he is also passionate about anonymous communications and anonymous voting systems. Chaum pioneered the ideas of a network of nodes that pass messages between each other in a way that cannot be tracked. This paved the way for programs like Tor to allow anonymous online web browsing by allowing users to connect to various nodes around the world, and pass their traffic among them in order to shuffle the data. Furthermore, in 1994, Chaum invented the first peer-to-peer voting system that allowed each vote to be cryptographically verified to ensure the that DRE does not modify the contents. This system was integrated into the Takoma Park, Maryland election in November of 2009.