The State of Cryptocurrencies, Their Issues and Policy Interactions

Ramesh Subramanian
Quinnipiac University
USA

Theo Chino
Bitcoin Entrepreneur
New York, NY
USA

Background: Early work on cryptography

As noted by William E. Burr, until the early 1970s, there was little commercial or academic expertise in cryptography (Burr, 2001). Cryptography and encryption were generally the preserve of defense establishments such as the military and the espionage agencies. Public awareness of cryptography in the US came with the publication of the Digital Encryption Standard (DES) on March 17, 1975 in the Federal Register (Leech & Chinworth, 2001). The origins of DES can be traced to 1971, when IBM researcher Horst Feistel, working on a project codenamed Project Lucifer, filed a patent application for a 48-bit block cipher cryptographic system (also known as the Lucifer cipher) (Feistel, 1974). The project was commissioned by Lloyds Bank for encrypting ATM transactions. In 1972, the National Bureau of Standards (NBS) identified the need for an
encryption standard for encrypting unclassified but sensitive government documents, and in May 1973, solicited proposal for such a system. The NBS then chose, with the approval of the National Security Agency (NSA), a modified version of IBM’s algorithm (IBM, 2012). The original algorithm was strengthened to a 56-bit block cipher by a team led by Walter Tuchman and aided by Carl Meyer (Bamford, 1982). Other members of the team were Don Coppersmith, Alan Konheim, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith and Bryant Tuckerman. On January 15, 1977, DES was adopted as a standard for unclassified government documents.

The publication of DES did led to many discussions and debates in the academic community and civil society. Some academics such as Martin Hellman and Whitfield Diffie at Stanford University felt that the original 56-bit block cipher was altered by IBM at NSA’s behest to provide that NSA a backdoor into the cryptographic system. They also felt that the 56-bit cipher was not secure enough and could be broken with appropriate computing power – presumably available to the NSA, again enabling it to capture and decrypt messages (Blight, 2013). The controversy made the DES standard one of the most scrutinized cryptographic systems. Diffie and Hellman conducted a comprehensive analysis of the DES in 1977 (W. Diffie & Hellman, 1977). However, DES became very popular and was soon adopted internationally as the encryption standard. This period also saw further developments in cryptographic systems. In 1976 Ralph Merkle developed a paradigm based on the concept of a “puzzle” to accomplish secure communications over insecure channels (Merkle, 1978), and at around the same time, Diffie and Hellman proposed a system they called “Public Key Cryptography” and thus developed public key encryption (Whitfield Diffie & Hellman, 1976).

The early controversy pertaining to DES serves to illustrate the sense of unease that the academic community and civil society had over the possibility of its misuse by the government to surveil citizens. This unease led some people to conceptualize the development of anonymous means of communications and anonymous methods of financial transactions. Developments in this sphere also occurred in conjunction with developments in network computing in the 1970s and 1980s, the advent of the Web in 1991 and the ensuing surge in web-based commerce. Along with this came the realization that a person’s online activities could be easily tracked by various entities (Narayanan, 2013a). This gave impetus to the emergence of cryptocurrencies – digital currencies whose movements could not be tracked easily (Narayanan, 2013a). Interest in creating alternate exchanges that are anonymous, fast, allowed direct peer-to-peer transactions without any intermediary grew. An autonomous digital currency that is not connected to any government or other intermediary such as a bank is appealing because of the anonymity and liberty that it affords. Transfer of money across geographic regions both domestic and international can be easily and quickly accomplished without worrying about governmental regulations.

These ideas coalesced into the Cypherpunk movement that “formally” emerged in the early 1990s. The cypherpunk movement (not to be confused with the cyberpunk movement) is an activist movement whose participants seek to engineer social and political change and subvert the status-quo by enhancing security and privacy through cryptographic techniques. The founders of the cypherpunk group were Eric Hughes, a UC Berkeley mathematician, Timothy C. May, a former chief scientist at Intel, and John Gilmore, one of the early employees (the fifth employee) at Sun
Microsystems and founder of Cygnus Support as well as the Electronic Frontier Foundation. All three were wealthy, and shared a strong libertarian streak. The group started with a meeting in 1992 in the Bay area of San Francisco. They started the cypherpunk mailing list in 1992 and within two years, the mailing list garnered over 600 subscribers.

An important technology enabler to this movement is David Chaum, a cryptologist who got his doctoral degree from the University of California Berkeley. As a doctoral student in the 1980s, Chaum explored several concepts and developed several methods focusing on anonymous communication and anonymous financial transactions. In 1981 Chaum published the article “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms” which described a method, using public key cryptography, to hide the identity of a participant in an email communication, as well as the contents themselves. He explained one of its uses - in elections where an examiner could verify that all the ballots have been correctly counted without revealing the identity of the voters (Chaum, 1981). His 1982 doctoral dissertation titled “Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups” (Chaum, 1982) and his 1983 paper on “Blind signatures for untraceable payments” (Chaum, 1983) laid the foundations for the creation of an anonymous currency. As early as 1985 he stated that “Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate.” He proposed an approach using which surveillance of electronic transactions could be rendered “obsolete (Chaum, 1985).” Chaum went on to create a digital currency based on cryptography that he called E-Cash, and in 1990 founded a company called DigiCash, an electronic money corporation. The world’s first electronic cash payment took place in May 1, 1994. However, most attempts at creating a workable cryptocurrency have failed to gain consumer acceptance. DigiCash filed for Chapter 11 bankruptcy on November 4, 1998. Since then, several new attempts have been made to create digital cryptocurrencies. Examples are Peppercoin – a company founded by Ronald Rivest and Silvio Micali that uses a cryptographic system for processing micropayments (Micali & Rivest, 2002); the NetBill, another system for micropayments for information goods from researchers at Carnegie Mellon University (Cox, Tygar, & Sirbu, 1995); Wai Dai’s B-Money which was a precursor to Bitcoin (Vigna & Casey, 2015, page 319, Note 51) and Nick Szabo’s Bit Gold (Szabo, 2008).

Despite this renewed activity, by 2013, many analysts had written off any future for these types of currencies. Arvind Narayanan and Jonathan Zittrain separately note the following points that make cryptocurrencies unusable in the long run (Narayanan, 2013a; Narayanan, 2013b; Zittrain, 2012):

1. They are extremely complicated for the common person to understand and use – the lay user may not have the technological familiarity to download and operate the necessary software and implement the necessary security measures required for cryptocurrencies.

2. Maintaining absolute privacy may not work economically in a world where collecting, aggregating and selectively disseminating personal data is a technique used by almost
all businesses – many businesses are able to provide “free” services to users only because they can collect, categorize and sell users’ information to advertisers or other aggregators.

3. The concept of trust without any government to back it might be unpalatable to many people – the lay person still accepts the authority of the government and the government’s guarantee on currency.

4. Many existing laws and legal restrictions such as the Digital Millennium Copyright Act (DMCA) will undermine such digital currencies – some of the proposed currencies could be stopped if they are found to violate the copyrights of other software.