Crypto and Currencies: ecash, fcash and zcash

C.E.Veni Madhavan
Department of Computer Science and Automation
Indian Institute of Science, Bangalore

Abstract

Cryptocurrencies, in particular the first and well-known Bitcoin and others such as Ethereum, are canonical examples of the blockchain paradigm. Minting or generating new elements or coins of this form of currency relies on the notion of *proof-of-work*. Generation of proof-of-work is based on solving a computationally intensive problem such as finding a specific form of hash string. Cryptocurrencies have serendipitously heralded a digital information revolution in the form of *blockchains*, a broad term, for distributed ledger technologies.

As monetary instruments these attempt to provide for the many attractive properties of *fiat currency*, such as privacy, anonymity, transferability, fungibility. However, these are different, from State backed denominational fiat currencies, with respect to the properties of *fixed, store-of-value, medium-of-exchange*, *arbitrage within jurisdictional boundaries*, *seigniorage in fiscal governance*, *taxation and law enforcement*. An alternative paradigm of cryptographic digital cash, the analog of fiat currency, in the form of digital coins, coupons or tokens, predates the contemporary examples of cryptocurrencies. Our work is on such a system of *virtual money*.

We discuss these paradigms of *cryptonomics*, covering instruments such as electronic cash (*ecash*), fiat cash (*fcash*), cryptocurrencies (*bitcoin, zcash*), from perspectives of science, technology, economics, applications, mathematics, governance and human-usage factors.