Financial Market Infrastructures and Payments: Warehouse Metaphor Textbook
Ron J. Berndsen

Answers to Exercises of Chapter 8

1. Cryptocurrency is defined in the textbook on page 128 as a digital asset used in a system as a medium of exchange where 1) there is no central authority involved to obtain the true state of ownership, 2) ownership transfer can be proved cryptographically, and 3) there is double spending prevention in place.

2. There are four problems that need to be solved by a cryptocurrency: the double spending problem, the money supply problem, the privacy problem and the peer-to-peer problem. See pages 126-127 for more information. The Traditional Warehouse solves only two of those problems (double spending and money supply) or even three (in case of banknotes it also solves the privacy problem). The peer-to-peer is not solved by the Warehouse but it also doesn't need to be solved as there is some trust in the central authority (being it a bank, other payment service provider, central bank or an FMI).

3. The unique selling point of Bitcoin is that it solves the peer-to-peer problem as you only need to trust the Bitcoin software but not a financial intermediary. This is however only achieved when peers are running full nodes.

4. Mining is essential in a trustless environment as proof that a certain block is a valid successor and that the bitcoins involved in that block have not been spent before.

5. The drawbacks of Bitcoin are the scalability problem (speed), the excessive use of energy, and the possibility of a 51% attack (see page 133).

6. The specific problems that Bitcoin Gold, Bitcoin Cash and Bitcoin Private are trying to solve are discussed in Table 8.1 and the accompanying text.