Lecture 11: Cryptocurrencies; The Industrial Economics of Banking

Section 10.4 deals with cryptocurrencies, which on the face of it seems to be monetary economics rather than economics of banking, since it deals with payments without financial intermediaries. However, there is much more to cryptocurrencies than just developing an alternative form of money, and the interest in the field, which was initially mainly directed towards BitCoin and its various successors, has now focussed on what could be considered as the “engine” behind cryptocurrencies, the blockchain technology. The blockchain was designed in connection with the launch of BitCoin, the first electronic currency but it has eventually found many other applications, and the blockchain technology is being adapted also by banks, both ordinary banks and central banks.

We begin with the construction of an electronic means of payment. The basic idea is that an agent should be able to transfer a unit of the currency to another agent digitally. In the BitCoin architecture, this is achieved by digitally signing coded message, a hash, of the previous transaction together with the public address of the other agent and adding this to the coin, which in this way takes the form of a long list of transactions. The procedure is illustrated in Fig.1.

FIG. 1. Transactions with BitCoin: The owner uses the public key and the hash of previous transactions together with a private key to sign a transfer. The last transaction is then added to the list of previous transactions.
This part of the problem, transferring money in a secure way from sender to receiver, is not new and not specific for the cryptocurrency. But there is another part of the problem, namely that of preventing double-spending, which must be solved, otherwise the same amount of money could be used again and again. The classical way of achieving this would be to have a central authority monitoring all transactions, but BitCoin instead uses a system of public announcement, so that all transactions are visible to everyone. For this to work, there must be an arrangement by which all eventually agree about a single history of transactions.

This is where the proof-of-work technique comes in: A number of new transactions are collected to form a block. Each block has a header containing (among other things) a hash of the previous block and a nonce, a 4 bytes array which is 0 at the beginning. To verify the block, an agent in the network must perform repeated trials and errors, each time increasing the nonce by 1, so that the hash of the other content of the header together with the nonce either obtains a prescribed value or differs from it by an allowable distance. Here the hash function is a given function transforming large data arrays to smaller ones in such a way that it is easy to perform a hash of a given array but very complicated to find an array which produces a given result. Once a solution has been found, the relevant agent publishes it, and everyone can verify that it is correct and that the transactions in the block are legitime. From now, the block can be used as parent block for new proof-of-work verifications.

![Fig.2. Verification of transactions ('tr.' in the figure) by proof-of-work: The header of the block, containing among other things a hash of the previous block, with the nonce appended, should result in a series of 0 when hashed. To obtain this, the nonce is changed step by step. When the result is obtained, the block is appended to the previous blocks as another block in the chain.](image)

The procedure is illustrated in Fig.2, where the block to the right is subjected to the proof-of-work verification. Once it has succeeded, the block is included in the chain and the transactions in the block can be considered as verified. This means that the acquirer of the BitCoin can use it in future transactions.

The main achievement of BitCoin, at least in our present context, is that it demonstrates the possibility of a totally decentral means of payment. The particular version of such a decentral electronic currency has some limitations (such as its small capacity, which has to do with the choice of block size, the particular proof-of-work
selected, which is energy-consuming when carried out on a large scale), but this need not detract us here: What matters is that totally decentralized transfers is achieved using the blockchain technology, which essentially can be reduced to keeping a publicly accessible ledger which shows all the transactions that have been carried out using the electronic currency involved. This presence of this form of memory is what allows BitCoin and the subsequent versions of cryptocurrencies to fulfil the role of money. This has actually given a new understanding of money as memory, something which however is far outside our scope,

We now move to Chapter 11 dealing with interbank competition. This is a long chapter and we split it in two parts,

(i) standard industrial economics in the financial sector, dealing with competition in interest rates or in amounts of deposits and loans,

(ii) the connection between competition as discussed in (i) and risk-taking, with its implications for the stability of the financial sector.

Clearly (ii) is what interests us most, and (i) can be considered as a warming up for what happens in (ii). In the present lecture we cover most of (i), leaving a treatment of monopolistic competition the next lecture.

The story begins – as always when discussing competition – with the textbook world of perfect competition. The latter means that all agents (banks) take the prices (interest rates) as given and beyond their influence, and they act accordingly. Since this is a far shot from reality, we should not go into much detail, the main point is to fix ideas and notation for what comes. Here it is worthwhile to focus on the equation for the bank’s profit just below equation (2) (I should have given it a number also), which is no big deal but nevertheless shows that the banking business splits into two, namely earning money by lending at a higher rate than the funding rate, and earning money by taking deposits at a lower rate than the funding rate. The reserve fraction $\alpha$ is mainly of interest for macroeconomists (it gives rise to the money multiplier in textbook macroeconomics, there is a comment on this in the box, but don’t feel obliged to read it), we shall use it only a few times in what comes.

Since there is perfect competition, it is clear that banks choose the amounts of loans or deposits so that marginal cost equals the net interest rate (taking into account the funding rate in the proper way). The further story about equilibrium in the market can be passed over quickly, after all perfect competition is not what we expect to see out there.

Having mastered perfect competition in this easy way, we move to the other extreme, a monopolistic bank. Again, despite its fancy name, nothing happens which was not already known from basic microeconomics, and the various ways of expressing the pricing formula (either as Lerner index or by Amoroso-Robinson) should also be
wellknown from previous courses, once again we may pass it over quickly. The same goes for the story about bank levies p.220 which may safely be skipped. It is however worth looking over the final part of the section, on p.221, where the model is extended to treat oligopoly in the Cournot sense, that is where the firms choose quantities (amounts of loans and deposits) knowing the impact on interest rates. As always, the Cournot oligopoly does not look very realistic, but its results are reasonable, and we shall exploit the model (or rather a slight extension of it) later in the chapter when we discuss risk-taking.

We read: Chapter 10, section 4, Chapter 11, sections 1-3.