Cybercurrencies and Blockchain

There are several reasons for being interested in cybercurrencies in connection with financial intermediation. 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 many 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.

There are two crucial details in a decentralized currency:

(1) Money must be transferred from one user to another in a safe way (meaning that one can be sure that the payment arrives at the right place). The first problem is mainly one of *cryptography,* dealing with transferring messages from one person to another in a way that cannot be captured by others. The simple cryptographic schemes involve a code used by both parties, but such codes are reasonably easy to crack if the same code is used by sender and receiver. The advanced cryptographical procedures used nowadays involve a public key, known by all, and a private key known only by the individual. This part of the problem, transferring money in a secure way from sender to receiver, is not new and not specific for the cryptocurrency.

The basic demand of an electronic currency 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,* more about this will come below) 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.

A very simple example of how the public-private key is the following: Suppose that Bob wants Alice to send a message which cannot be read by anyone else (this is the standard setup in the cryptographics literature).

Bob chooses a *public key* (N, e), where $N = pq$ for p and q prime numbers, and e a positive number

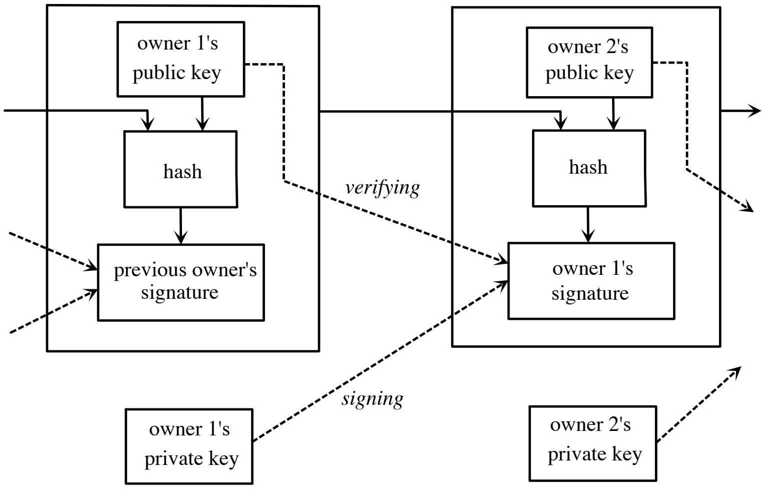

Fig.1. Transactions with BitCoin: The owner uses the public key and the hash of previous transactions together with a private key to sign a transfer. The last transaction is then added to the list of previous transactions.

such e, $p-1$ and $q-1$ have no common divisor of is 1.

Alice has a message which we assume converted to a number m between 1 and N. She uses the public key to compute c as the remainder after dividing m^e by N. For this Alice doesn't need to know p and q.

Alice now sends c to Bob, who then finds Alices's message from $m = c^d$, where d such that $ed \equiv= 1$ modulo $(p-1)(q-1)$ (this is a relatively simple problem for a computer).

All the way the key has been known only to Bob, the public key has only the number N, and if this number is large, finding p and q is a near-to-impossible task.

(2) the *double-spending* problem should be solved in a satisfactory way, so that the receiver of a payment can be sure that the sender actually had the amount which was transferred.

The other problem, prevention of double-spending, must be solved, since 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 and guaranteeing their correctness. These data could in principle be stored in any possible way, but a simple and relatively cheap way of organizing this is in the form of a chain of blocks, each containing a number of transactions. The authority can then collect new transaction data, control them and transform them into a new block added to the already existing chain.

So far the blockchain has been only a way of organizing a database, but for a decentralized currency it becomes a fundamental ingredient. A currency having to central authority must rely on a public database, with all transactions visible to everyone. Clearly, the blockchain construction is central here, since typically only recent transactions are of interest. But for this to work, there must be an arrangement by which all users agree on the correctness of the data in the blocks. We outline this below in the case of BitCoin. Once a procedure has been established for the approval of a new block, the remaining details can be organized as with a centralized currency.

For what follows it is useful to introduce *hash functions:* A hash function transforms a long string of data to a much shorter one (much like zipping a computer file). But the hash functions used here has crucial properties, in particular (a) changing the input of the hash function only slightly will result in very fundamental changes in the output, and (b) performing the action of the function (i.e. hashing a string of data) is reasonably easy and quick, but the reverse problem (finding a string which gives rise to a particular output) is very tough indeed. The hash functions used in practice mostly origin in number theory, related to prime number decomposition (easy to check but very time-consuming to find) or points on elliptic curves.

The hash function can be applied repeatedly, and indeed this is what is done when construction a block: Pairs of transactions are hashed into one string, the resulting strings are collected pairwise and hashed, and so one, until it all ends in one string, called the Merkle root of the block. It is seen that changing one single transaction means that all the many hashes are changes in a very conspicuous way.

BitCoin uses what is called a *proof-of-work technique* to approve now blocks: A number of new transactions are collected to form a *block*. All the information in the block is hashed repeatedly so as to obtain a Merkle root. Now the agent verifying the block (called a miner) must find a *nonce*, a string of fixed length, which if added to the Merkle root and hashed gives an output string with a preassigned number of 0s (the number of 0s depends on how difficult it should be to find this nonce). There is no other way of solving this problem than by trial-and-error, and it takes some time to do so (at least 10 minutes). This nonce is written into the block which is then finished, and the miner receives a number of currency units as a remuneration. Notice that once found, anyone can check its correctness just by performing the hashing. From now, the block can be used as parent block for new proof-of-work verifications.

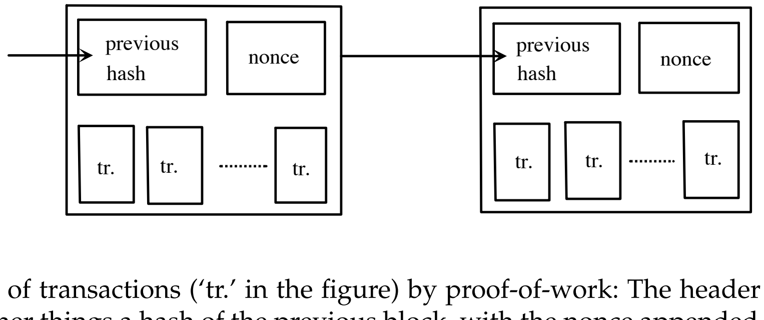

Fig.2. Verification of transactions ('tr.' in the figure) by proof-of-work: The header of the block, containing among other things a hash of the previous block, with the nonce appended, should result in a series of 0 when hashed. To obtain this, the nonce is changed step by step. When the result is obtained,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

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 cybercurrencies 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,