The Economics of Digital Documents

Mauro Cipparone
mcippa@netnerds.prestel.co.uk
http://www.geocities.com/WallStreet/2486

Mauro Cipparone has recently graduated summa cum laude at LUISS university, Rome, with a thesis on the economic consequences of Internet payment systems. He collaborates with the computing center of LUISS university, Rome, and with the association "Liber Liber," occasionally giving lectures on Internet payment systems.

The recent advances in the use of cryptography for authentication purposes could radically change the way our economy works. Such a change particularly affects the way wealth is transferred between individuals and circulates within the economy.

Such a change would derive from the possibility to forge digital documents incorporating rights and/or duties. This could allow the digitalisation of many instruments which currently rely on paper for their circulation. Such instruments form the backbone of today's economic activity. Their digitalisation could open up new opportunities and challenges, if some technical and theoretical problems can be addressed and solved. The biggest one is probably what I would define as the "uniqueness problem". A paper document is far harder to reproduce than a digital one. A digital document is a sequence of 0s and 1s. As such, it is trivial to reproduce the same sequence over and over again. It is beyond the purpose of this article to discuss the approaches to solving this problem. I will assume that in the future it will be possible, via a hardware and/or software solution, to produce digital documents that cannot be easily copied and counterfeited.

We can imagine a wide variety of documents which could be digitalised. Currently, attention is focused mainly on payment instruments, such as electronic cash and electronic cheques. But the protocols which are currently being developed to handle such instruments could later be adapted to different uses.

What is an electronic coin? It is a digital document, containing the promise to pay to the bearer on demand a certain fixed amount of money. Under this respect, it can be viewed as the correspondent of today's (paper) travellers' cheques, a slip of paper containing the promise of the bank issuing them to redeem them at their nominal value on demand. An electronic cheque is a document containing the promise of a banker to pay a certain amount of money on demand. Current paper cheques are part of a wider class of instruments, called bills of exchange.

A **bill of exchange** is "an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay on demand, or at a fixed or determinable future time, a sum certain in money". Whereas today the attention is focused on cheques, nothing prevents the issue of digital bills of exchange of different kinds. Digital bills could be digitally signed, endorsed and transferred just like paper ones.

Another class of documents which could be digitalized is shares and bonds. To put it in the simplest way possible, a share is a certificate, signed by a company, granting its owner certain rights and obligations. Bonds are documents acknowledging the debt of a company towards the owner of the bond.

In civil law countries, all such documents fall in the wide category of the **"titles of credit"**: the document is not a mere acknowledgement of the rights and obligations it describes, it "incorporates" them. The transfer of the document thus implies the transfer of the rights incorporated. From here onwards, I will refer to such a notion, which is more general, and which I know better.

Titles of credit were originally created to make the transfer and negotiation of the wealth they represent easier. Modern economic life would be impossible without them: it is through such documents that entrepreneurs can obtain large amounts of money for long periods of time for their investments, while the investors can mobilise and negotiate their shares in such investments, without having to commit their wealth for all the time span of the investment. Using titles of credit solves many problems which prevent the circulation of wealth. If the transfer takes place using a title of credit/bill of exchange, it is only necessary to check the validity of the document to be sure to obtain the right it incorporates.

More recently, however, titles of credit have started to show their limits. Today's transactions use information technology which is incompatible with the physical transport of paper documents, which is slow and risky. Legal systems have adapted to a certain extent. However, many operations still require actually showing the document or signing it. This causes lots of problems and hassles, especially for stocks and bonds, which can be transferred between people in different cities or countries. To solve these problems, a huge and complex infrastructure of intermediaries has been built. Normally, the paper documents are physically held by some depositee, public or private, which manages them. Sales and purchases are then regulated through crediting and debiting share and debt accounts. Intermediaries don't only handle the paper documents. They also manage the risks which arise from handling such a complex infrastructure.

Before the dematerialization of documents, it was possible to deliver the documents at the time of payment (delivery vs. payment), or shortly thereafter. Investors would send their shares and bonds to the city where the nearest stock exchange was located, and physically give the documents away after negotiation. Today such agreements are impossible, because shares and bonds can easily be sold to investors in other countries and continents. This means that, despite the advances of information technology, it is impossible to check in real time that the buyer of some stock actually has the funds, and that the seller actually has the stock. In those stock exchanges in which "regulation" (the actual entries in the books which document the transfer of money and stock) only takes place once a day or once every few days many investors take advantage of such time lags to sell and buy without having any backing for their operations. Such operations are normally discouraged, because they give rise to risks which can be taken into account of with difficulty: in any of these operation there is a "hidden" loan. Such risks are the reasons behind the capital requirements for firms that want to operate on the stock exchange, and for many other regulations.

I believe it is really a bottleneck problem: all the millions of operations taking place in the stock exchange eventually need to be regulated with double entries in the books of only one or very few clearing institutions. Even payments are cleared, at an interbank level, only by one or very few institutions (typically, using the accounts the banks hold with the Central Bank).

I think that the great revolution that digital certificates allow will make change possible, if not likely. Until recently, the only way electronic transactions could take place was through double entry bookkeeping. This necessarily requires a centralised structure to settle the transactions. On the other hand, digital certificates allow a return to the simple transaction model of the past, that is to say delivery vs. payment, but using the speed and efficiency of computer networks.

If the "uniqueness" problem will be solved, no longer there will be the need of using accounts to handle financial transactions. A stock exchange could then be a very simple institution, not significantly different from an Internet mailing list. Offers would be posted and retransmitted to all investors. Some mechanism would allow the match of compatible offers. Then, the seller and the buyer would simply send to each other the digital bond or share, and receive the digital payment. No intermediary would necessarily be involved, the transaction would be cheaper and systemic risk would be substantially eliminated. Eventually, the exchange of shares and payment could be made simultaneous by using a server trusted by both parties, who would release the shares only when the payment was sent to the server (who would then forward it to the seller).

Furthermore, digital bonds and stock could be managed much more cost-efficiently than paper ones. As an example, dividends could be managed by computers, who would simply send the digital coupons to the issuer of the stocks, and receive in return a digital payment. But the digitalisation could also allow completely new opportunities. For instance, governments could issue bonds in the form of encrypted coins. At maturity, the government would simply release the

key to unlock the coins, a very cheap alternative to the expensive infrastructure needed to manage bonds.

The consequence of digitalisation is ultimately a strong spur towards decentralisation and disintermediation. If it takes off, the institutions which supervise and control the financial world will find it harder and harder to fulfil their duties. Even capital movements could become much harder to prevent or even detect. If wealth can be kept in the form of digital certificates stored on a hard disk, then it can be transferred with the only need of a modem and phone.

Is such a scenario likely? Whereas before the invention of "digital signatures" it was technically impossible, it is now at least feasible. I like to think that cryptography can be compared to the invention of the printing press. Some financial instruments, which were not even conceivable without the possibility to print cheaply vast numbers of documents, became possible. It has taken centuries before they were actually invented, and centuries before they became widely used and available. Similarly, it is unclear how long it will take for the technology to take off and for the people to adapt to it. It is further unclear whether governments and the powerful interest groups which manage today's financial system will oppose such changes. Just like with the printing press, it is still possible to censor books, but the printing press cannot be dis-invented. And sooner or later, someone will use it.