DeNederlandscheBank
EUROSYSTEEM

If Blockchain is the answer, what is the question?

Ron Berndsen

De Nederlandsche Bank

Speech at the Dutch Blockchain Conference, 20 June 2016

In 2011 a breakthrough in information technology took place: A computer beat two human contestants in Jeopardy, a famous American television quiz in which the answer is given but the contestants need to come up with the relevant question. Let's do Jeopardy: *If Blockchain is the answer, what is the question?*

Advances in information technology are not only relevant for Jeopardy, they are also a major driver for the development of the blockchain technology. Increasingly central banks view blockchain as a potentially promising technology for financial market infrastructures, but much less so for virtual currencies. Given its experimental status my remarks on blockchain today - or distributed ledger technology if you want[1] - are preliminary. It will take a number of years before the full potential will become clear.

Why are central banks interested in blockchain?

[1] For convenience in this speech, I will use the term blockchain rather than distributed ledger technology.

The fact that digital currency in the form of Satoshi's bitcoin was the *first* blockchain application has been a blessing in disguise. Initially the potential benefits of bitcoin were outweighed by negative publicity, such as the association with semi-legal activities and the bubble-like price increase in 2013. And indeed De Nederlandsche Bank (DNB) deemed it necessary end-2013 to warn the general public for the risks of bitcoin. However, since bitcoin challenged to some extent the notion of money – bitcoin is usually referred to as a virtual currency – it also triggered interest to further explore the underlying technology. I doubt whether central banks would have done the same if the first application of blockchain would have been, for example, in health care. DNB is interested because blockchain may have implications for the overarching goal of financial stability and her three primary tasks: 1) promote the smooth functioning of the payment system, 2) prudential supervision and oversight and 3) monetary policy.

So, for the first central bank task, smooth functioning of the payment system, the blockchain is a promising technology for financial market infrastructures. Financial market infrastructures serve as the backbone of the economy for settling complex financial transactions in a network of participating banks.

For the second central bank task, prudential supervision and oversight, the blockchain technology might potentially add a new dimension to the interaction between the supervisor and the supervised institutions: if they share a blockchain the supervisor can automatically see all verified transactions.

For the third task, monetary policy, it is necessary to understand the potential implications of blockchain for the money supply and potential seigniorage consequences of virtual currencies. In short, for all three central bank tasks it is important to increase our understanding of the benefits and risks of this new technology.

Why DNBcoin?

So last year we started our DNBcoin experiment. The general idea was that by adapting the Bitcoin software ourselves we could learn deeper how an actual implementation of the blockchain really works than if we would only perform desk research and go to conferences such as these, no matter how interesting. And just to avoid misunderstandings: the DNBcoin is only developed for internal test purposes, it will not be put into circulation. For the experiments, we didn't establish a traditional steering committee with working groups, mandates and budgets; we just formed a bootstrap team of intrinsically motivated colleagues coming from different parts of the Bank. If you work on innovation, you should work in an innovative way as well.

We adapted the bitcoin client software in two major ways. DNBcoin prototype 1 was basically replicating the early days of bitcoin (Jan – Feb 2009) using five laptops in a connected network and our home-made genesis block. We were able to generate a couple of thousand blocks, to enter transactions and set transaction fees. We also established that you could easily mine blocks too quickly: every 3 minutes instead of every 10 minutes like bitcoin. Reassuringly the software then issues the warning "abnormally high number of blocks generated in the last four hours".

The second DNBcoin prototype takes the other extreme of bitcoin by jumping to the year 2140, the year when the last fraction of the 21 million bitcoins will be issued. This maximum follows mathematically from the halving of the issuance of new bitcoins every 210,000 blocks, starting from the initial reward of 50 bitcoin per block. As you probably know the next halving of the bitcoin block reward – from 25 to 12.5 BTC - will take place in a couple of weeks from now. We thought that the second prototype would therefore be a so-called pre-mining variant. All DNBcoins would be mined first by only one laptop before opening the network to the other laptops. To minimize power consumption, we have started with an initial block reward of 1 billion DNBcoins in the first block and a very high frequency of halving that reward, namely every two blocks. In doing so we were able to generate 3 billion DNBcoins in 30 seconds. In addition, we observed that after all DNBcoins had been generated, blocks could still be mined and added to the blockchain. The reward was reduced to zero but transaction fees were still collected by the miner who finds the next block.

These two prototypes were focused on the blockchain as a vehicle for a virtual currency. But virtual currencies are not the most promising application of the blockchain. So the third DNBcoin prototype will not be about a virtual currency. Before I come to that, I will first go into the essence of blockchain technology. As with any new development, definitions are not commonly agreed yet, so I should make clear what I see as blockchain technology.

When can a technology still be considered Blockchain?

The concept of blockchain for bitcoin was clearly aimed at a specific problem: build a digital currency for a trustless network without double spending. In other words, how to exchange digital currency with people you have never met but be sure you don't get a counterfeit digital coin. I won't go into the issue whether that problem is really solved but we can agree it is a specific problem indeed. This however begs the question: If we depart from the bitcoin concept of blockchain, how do we know it is still blockchain? I hear often that blockchain is merely a distributed database or an application of public key infrastructure.

So what *is* a blockchain? It is possible to decompose the blockchain in its underlying technologies, and I think there are three fundamental pieces of information technology involved: 1) public key infrastructure, 2) fault tolerance and 3) consensus algorithms. First, public key infrastructure[2] provides ownership of the data i.e. if you know the private key you can transfer the asset, and tailor-made transparency (who may see what?). Second, fault tolerance delivers resilience of the network. It doesn't matter if some nodes of the network are temporarily unavailable or compromised, as long as some nodes keep working, the network is protected against outages and malicious attacks. Third, the consensus algorithm establishes the truth of the information in the network.[3] If there is consensus about the validity of a new block, it is added to the chain. Having outlined what I consider to be blockchain technology, I now turn to the potential of the blockchain.

[2] Developed by Whitfield Diffie and Martin Hellman (1976).

[3] See Ben van Lier (2016) who argues that the earliest predecessors were proposed by Leslie Lamport as Byzantine fault tolerance (1982) and the Paxos consensus algorithm in 1990.

What is the most promising area of application for blockchain?

Currently, the most promising area of application for blockchain, and probably the direction for the third DNBcoin prototype, is in environments with the following four properties:

- The network is about ownership of a certain digital asset;
- There is some degree of trust among participants in the network;
- Resilience of the network is crucial;
- Adding intelligence to initiate or trigger transactions is important

I would now like to discuss these points a bit further. The first one, ownership of a digital asset defines the scope. Blockchain could be suitable for networks designed for registration of ownership of a digital asset and transfer of that ownership: from a financial-market-infrastructure angle we are talking about settlement of transactions and custody of assets in a distributed ledger. A fundamental property of a distributed ledger is that local reconciliation of transactions is no longer needed. Digital asset is to be understood here in a broad sense. Examples include financial assets such as bonds, derivatives or fiat currencies but could also refer to property rights in real estate. The main point is that "double spending" or counterfeiting of the digital asset is prevented: it should be impossible to include a copy of the digital asset with precisely the same characteristics and time-stamp in the blockchain.

The second property, some degree of trust, means that there should be at least some trust in the network in the sense that the identity of the participants is known. With known identities it becomes possible to verify ownership of the digital asset at each point in time since the blockchain is time-stamped. The requirement of some trust in the network makes the problem easier to solve than the harder problem of a completely trustless network. Hence this is computationally an easier requirement than the trustless network of bitcoin, which necessitates a resource-intensive proof-of-work algorithm.[4] Blockchains without intensive mining but with an alternative consensus algorithm could probably be

[4] This type of proof-of-work algorithm, called hashcash, is developed by Adam Back (1997).

made fast enough to handle a high-volume of transactions. On the one hand, full anonymity for everyone is not desirable in transfer of ownership given know-your-customer and anti-money laundering legislation. On the other hand, it may be desirable to have some degree of privacy: you may see your own transactions but not those of other participants and some participants such as the operator and prudential supervisors can see more. The technology should be flexible enough to strike the right balance between privacy and transparency.

The third property is about resiliency of the network. This point is often overlooked but in my view resilience of the blockchain is potentially a very strong point. In terms of operational resilience, a blockchain where every node has the full ledger makes such networks less vulnerable to a natural disaster or targeted attack than the customary two or three data-center configuration. But also in terms of cyber resilience, due to its cryptography-by-design nature, the blockchain may be an improvement over existing systems: time will tell. Furthermore, if the consensus rule in a particular blockchain requires a large majority of nodes that are active to agree on a certain transaction, it becomes also harder for the malicious insider to commit fraud.

The fourth and last property is about adding intelligence to the blockchain, sometimes referred to as smart contracts. They can be loosely defined as a set of rules that may fire upon the fulfillment of certain conditions. A smart contract is in that sense able to enforce itself. In so doing new transactions may be created or predefined transactions may be triggered by such contracts. Here it is also important to underline that the node in the network does not necessarily have to be a separate legal entity or a mobile device in the hands of a natural person: it could be a machine as part of the Internet of Things.

All these characteristics taken together suggest that blockchain may be naturally applicable in the field of financial market infrastructures which take care of the settlement of complex financial transactions.

What are the barriers for adopting blockchain?

However, there are also barriers to overcome if blockchain is to be the new technology for financial market infrastructures. The barriers are not new but if blockchain is to succeed there is a need to overcome them.

The first barrier is fragmentation: many institutions are developing their own variant of blockchain. A good way to overcome this barrier is to adopt a worldwide standard for blockchain. The standard should be open source and sufficiently detailed in order to allow exchange of information between blockchains, where permitted. Some initiatives are already underway but no doubt further experiments are necessary.

The second barrier are vested interests. In the current payments and securities landscape there are a large number of market players whose business model is, partly or wholly, based on existing inefficiencies. If blockchain becomes a successful technology the need for some intermediaries will disappear. A likely condition for this to happen is an order of magnitude reduction in costs of total ownership. Only then will some existing market players be willing to invest in this technology.

The third and last barrier is interoperability. In network industries the lead time for renewing the infrastructure is measured in years, not months. This implies that the adoption will be gradual. Interoperability between existing systems and blockchain implementations is needed to make sure that the current settlement and custody activities can continue at all times. Disruption at the level of financial market infrastructures is not so likely.

If Blockchain is the answer, what is the question?

Let me conclude. History teaches us that when looking ahead into the distant future, it is wiser to predict that something is possible, rather than that something is impossible. The blockchain technology offers a number of advantages over existing technologies. But there are also some drawbacks and barriers to overcome.

Well it is high time to finish our game of Jeopardy. The winning question I would endorse today with the answer “blockchain” is… “Which technology for the next generation of financial market infrastructures?”

Thank you for your attention.