The need for a legal tender digital money

Prof. Massimiliano Sala

University of Trento

Milano, 27^{th} May 2015

Digital money system

The principal components of a digital money system are two:

1. digital money issuing (the equivalent of *money printing*)
2. digital money transactions

Traditional digital money system

1. Issuing is done by the Central Bank that gives the money to Retail Banks that may give to other operators and, eventually, digital money arrives at a user's *account*

2. Transactions are performed by a very complex network called a *circuit*

Bitcoin-like digital money system

1. Issuing: some (unpredictable) mathematical algorithm, involving randomness, will issue banknotes from time to time

2. Transactions are very efficiently handled by a shared balance sheet (*block chain*) and automatically verified by digital signatures (elliptic curves)

The value

The value of a digital money is given by its **acceptance**.
Examples:

- at 18:49 of yesterday, one bitcoin equals 218,40 euros;
- if you have 10 euros in your credit card account and you are in a shop with no POS, the value of your digital euros is zero;
- currently a 10-euro lunch ticket in Trento is accepted as 9 euros by many merchants;
- if you go to a shop with a 10-euro banknote, it is accepted as 10 euro;
- if you go to an Italian shop with a one dinero coin issued by Billostan, it value is zero.

The value

We claim that the value of digital money is given by:

$$\frac{\text{intrinsic value created by issuing}}{\text{cost of transactions}}$$

Let's come back to cash

The intrinsic value created by issuing depends on the **trust** that you give to a currency, which in turn depends on:

- the strength of the country issuing the currency;
- the total amount of banknotes;
- some mysterious factors related to our emotional state (we are humans after all!).

Last slide on cash

The cost of transactions in a **cash-only society** is hidden to the common citizen, but it is huge:

- money needs to be printed (isn't this issuing??);
- money needs to be distributed to retail banks by the Central Bank, with very high security;
- money needs eventually to be given to the citizens (again with high security);
- counterfeit money must be continuously searched for, identified and removed from circulation.

Most citizens are unaware of all these problems, but they are hotly aware of the need of physical proximity for exchanging cash. We claim that this is the **highest cost** (from a global system point of view).

Intrinsic value of issuing by a country vs. bitcoin

Leaving apart emotional factors and nominal values, the intrinsic value (in issuing) of a currency is given by the strength of a country.
But observe that a country needs a strong government and a strong economy **anyway**.
So the huge cost of having a strong country is taken for granted, but it is this cost that makes a currency strong.

What is the intrinsic value of a bitcoin when it is issued is much less clear.
What is the country backing bitcoin?
We will come back to this once we have discussed transaction costs.

The cost of transactions

In the three systems under consideration, where is the transaction cost?

- in a cash-only society, the physical (secure) moving of money;
- as regards **digital money**, the cost is mostly on the merchant side, who is so vexed by fees that sometimes he refuses acceptance (e.g., POS-less shops) and sometimes he makes the user pay more the same good;
- in the bitcoin network, the transaction cost is close to zero (this cost is so marginal that we will neglet it from now on).

Shops in Trento

There are shops near Trento that accept bitcoins but **do not accept** credit cards or other traditional digital money systems.
And this because of the (nearly complete) absence of fees for the merchant!

But of course there are many more shops that do the opposite.
And there are also shops that accept only cash (again, due to the fees).

The first case is an alarm bell for the traditional digital money system.

The intrinsic value of bitcoins

We have an intriguing paradox here.
If no Central Bank issues bitcoins, where is their value coming from?

Their value comes from some special uses (anonymous transactions in the black market inside the deep web) and the fact that their transaction fees are (close to) zero.

Usually, the acceptance of a (cash or traditional digital) currency is pushed by the strength of a country and halted by the transaction cost

However, for bitcoins it is the other way round (!), their value comes from their acceptance.

How can bitcoin transactions be so cheap?

In my opinion, the most stunning idea from the genius that we call Satoshi Nakamoto is to replace the trust on a system managed by humans (Central Banks, other banks, payment circuits, regulators, etc) with the trust on cryptography.

The entire bitcoin system is guaranteed to accept only valid transactions if and only if the inner cryptographic primitives are computationally unbreakable.

By replacing *human control* with cryptographic checking, Satoshi has killed transactions fees.

Do you believe in fairies?

Every year, new students in Cryptography ask me:

> Prof. Sala, do you believe that the cryptographic algorithms used nowadays are actually robust and not breakable?

My answer is:

> I don't believe in fairies.

Mathematics (and hence Cryptography) is not a faith and **needs no belief**, mathematics needs proofs.

The bitcoin curve

One of the essential cryptographic components of a bitcoin transaction is the so-called **bitcoin curve**, which is a mathematical object that guarantees that bitcoins are spent by the legitimate owners (of the corresponding eWallet).

There is no mathematical proof that the bitcoin curve cannot be broken (in a cryptographic sense).

Even worse, there is **no** curve that can be proved to be unbreakable (or at least that's what the academic community knows).
We do know **weak curves**, that can be broken easily, and we know suspicious curves, that have been created in an undocumented way.

What if the bitcoin curve is broken?

It is possible that, while we are speaking, a colleague in a university somewhere is finding a fatal weakness in the bitcoin curve.
Once her results become public, the trust in the bitcoin will go to zero and so will the bitcoin value!
However, past transactions will still remain safe (unless someone breaks also the hash functions, but that's another story).
What would kill bitcoin in this catastrophic event is the lack of a Central Body that has the authority to force the adoption of a new curve for new transactions.

Summarizing

Bitcoin is cool because it has transactions fees close to zero.
Someone thinks that Bitcoin is even cooler because they don't need to trust someone, they need only to trust mathematics.
But the fact is, mathematics cannot be trusted in the way they think, because the cryptographic primitives underlying bitcoins might be broken any time and the lack of a central authority would make their replacement very difficult and controversial.

A legal tender digital money?

My conclusion is that traditional digital money system cannot compete with bitcoin-like systems, because of the transaction fees problems. On the other hand, the lack of a central authority makes the bitcoin system extremely vulnerable.

What the world would need now is a digital money system that incorporates the advantage of traditional money (having regulators with enforcing powers) and the advantage of bitcoins (having zero transactions fees).

Conclusions

My belief (or wild guess if you prefer) is that we will soon see legal tender digital money appearing that incorporates many of the technology advances brought in by the bitcoin revolution, under the umbrella of respectable institutions.

How this new money will be is something I cannot predict but I can't wait to see.

Thanks for your attention

maxsalacodes@gmail.com