Bitcoin in Development and the Aid Sector

Bastiaan Quast

January 7, 2015

Abstract

The internet impacts virtually everything around us, the first half of this decade has finally seen that impact extend to the financial sector. we discuss two recent innovations in financial technology - Bitcoin and crowdfunding - in relation to the aid sector. Many aspects of Bitcoin are very enabling, which provides the development sector with a powerful tool for the achievement of its aims. In this context we discuss i.a. remittances, mobile transactions, and barter currencies in times of financial crises. Furthermore, potential uses in the development sector itself that we discuss are, accountability via the public ledger system, a lower threshold to online funding, due to the pre-paid nature, and a lesser dependence on local governments.

1 Introduction

Bitcoin is a online decentralised monetary system, which aims to cut out many of the middle men in the financial system, specifically governments and banks. The system is set up to be completely anonymous and decentralised, it originates from a white paper "Bitcoin: A peer-to-peer electronic cash system" published under the pseudonym Nakamoto (2008).

This article focuses on potential uses of Bitcoin in development and the aid industry, a discussion of the merit of the existence of the Bitcoin system is outside the scope of this article, we observe that for better or worse, the system now exists and will exist, although Bitcoin might be overtaken by even other systems, for the purposes of this article, we are primarily concerned with the fact that an anonymous internet-based transaction mechanism exists.

The ownership of bitcoins is registered in the public ledger called the blockchain, and can be proven by publishing a signature online, using a secret key. This means that transactions can be conducted from any computer or smartphone with internet access without a third party being needed.

There are many uses for a monetary system of this type, in this article we will focus on the uses particular to the aid sector.

In the next section, we discuss the mechanics behind the Bitcoin system in some more detail, with examples specific to development, as well the value of Bitcoin. Subsequently, we list some of the key potential uses of Bitcoin in the

development. In section four we discuss some new possibility for the aid sector in particular. We conclude with a discussion on the key challenges for widespread use of bitcoin in development and some recent innovations with potential uses in the development sector.

2 How does Bitcoin work?

Bitcoin was created in an attempt to solve the problem of online anonymous transactions in a decentralised system. This required addressing several previously unsolved problems. Bitcoin introduces several technological innovations.

The core part of the Bitcoin system is the public ledger called the blockchain, it contains all transactions in the history of the Bitcoin system. However, since the system was designed to be decentralised, there is not one primary version, in fact there are millions of identical copies called nodes. Decisions are based on a consensus of the nodes, which means that the majority determines which transactions are valid. This prevents individuals from meddling with the ledger.

The software that users have on their computer, phone, or online, is set over several keys. Most importantly, the private key, possession of this number constitutes ownership of the wallet. Using the private key, two things can be created, Bitcoin addresses, on which, bitcoins can be deposited, and digital signatures, which can be used to send Bitcoins from these addresses. A typical process would be as follows. A user downloads the Bitcoin software on his computer or smartphone. Using the software, a new private key is generated. Using the private key, a set of Bitcoin addresses is created. The users receives a Bitcoin payment in one of these addresses, in return for e.g. goods sold. The user now purchases something with Bitcoin. Using the software, a transaction from the Bitcoin address which received the Bitcoin is created and published to the Bitcoin network, in combination with a signature, which is also generated from the private key. The Bitcoin network receives the transaction request, using a mathematical procedure, the signature is verified to belong to the address containing the Bitcoins (this is proves that the signer owns the private key which belongs to the address and can be done by the network without knowing this private key). The transaction is then accepted at which point it simultaneously is committed.

It is useful at this point to make the distinction between Bitcoin (capital B), which is the entire system, and bitcoin (miniscule b), which is the dominant unit of account, similar to a Swiss franc or a euro.

Bitcoin Value

In the context of Bitcoin, the discussion of where it values derives from and the fact that is it not legal tender.

The discussion on it value is a complicated one, outside of the scope of this article. We will however make two observations:

1. Bitcoin has sustained a positive and large value over a sustained period of time

2. Most transaction unites in monetary systems, have no intrinsic value, fiat currencies, but even gold has very little

For a further discussion of Bitcoin and its value see Ron and Shamir (2013).

The issue of legal tender is quite different. Legal tender essentially means a state imposing a method of transaction (that it controls) within its territory. This has the positive effect that it unifies accounting. However, if the state does not manage the currency in a credible fashion, then this will lead to hyperinflation. This in term will lead to capital flight. A recent and reoccurring example in Argentina, which, at the time of writing, taxes all foreign credit card purchases with an additional 35%. By having a system without a single owner, this is rendered impossible. The Argentinian case further illustrate how Bitcoin can be used in times of economic crisis. During each of the currency crises that hit Argentina during the last decades, barter currencies arose. These provide a more stable means of holding value than government sanctioned money. By having a barter currency with a value outside the country (which can be quoted in US dollar), additional stability can be added.

3 Bitcoin in Development

There are many (potential) uses of Bitcoin in the development sector. An obvious first for a truly global and location independent monetary system is remittances. Transactions are virtually free-of-cost, and distance plays no role. The only requirement is that there exists a market where Bitcoin can be traded for local currency, which holds for most currencies.

However, even if such a market would not exist, there is to potential for communities to accept bitcoin as tender, in addition to existing forms. In particular, mobile payment systems using either smartphones or sms-based systems would make this particularly convenient.

4 Bitcoin in Aid

- traceability
- disbursement problem
- asking for direct funding, i.e. not through aid agency
  - lesser political liability, link to:
- subversive funding (high powered social media)
- problem of required internet access

In this section we will discuss how Bitcoin relates specifically to the aid sector, there are a few aspects of particular interest to the aid sector. Firstly, there is the instant nature of the transactions, and how this can help in possible disbursement problems. Secondly, traceability and anonymity of the transactions and how this relates to partnerships with local governments. Thirdly, in relation to local governments, there is the issue of not using the local currency, which is legal tender, which can be problematic if government disagree with this practice, but in situations where there is no cooperation it can also be beneficial, such as Argentina or Zimbabwe.

The second aspect of Bitcoin which is particularly relevant is the nature of the transactions. All transactions are public, as they are recorded in the public ledger called the blockchain, however originating and receiving addresses can be anonymous and created freely.

Traceability with local partner agreement, can be a condition for future cooperation. The optional message. Without local cooperation, the flow of Bitcoins can still be traced but it will not longer be possible to link addresses to individuals or organisations.

Anonymous donations to local partners, no need for government cooperation, also provide possibility of donating to readers, without directly embracing.

Crowdfunding and Bitcoin

A further recent innovation in the finance industry is crowdfunding. In a crowdfunding campaign an idea is described and the public is asked to 'donate' an amount in order to fund the realisation. Depending on the amount 'donated' this can unlock certain perks, such as: a thank you on social media, or a physical or digital copy of the final product, such as a video game or, a smartwatch (Pebble). Many of these campaigns have goals that involve social development, such as the Keepod campaign. Which aimed to create USB key which contains an operating system that can be loaded direct from the USB key, so that people who do not own a computer can run their own system on any computer. Contributors in this campaign could donate money, for each key that was ordered, an additional key was given to slum dwellers in Nairobi.

Generally these campaigns are organised through established platforms such a Kickstarter of Indiegogo. There are several reasons for this, firstly, payment if often via creditcard, which means that the institution has to be trustworthy. Since Bitcoin operate on a sort of pre-paid model, such as PayPal, it enables the customer to contribute without surrendering sensible information. A good example of a crowdfunding initiative that uses Bitcoin, is called "Bitcoin against Ebola", which provides books and lunches for children living in affected areas.

A variation on crowdfunding is the relatively recent phenomenon of internet tipping, like it's physical world counterpart, a good dead, idea, or comment is rewarded (after the fact) with a tip. By operating on a pre-paid model, tips can be given to total strangers, who otherwise would perhaps not be trusted with this kind sensible information.

5 Challenges and Future

What are the challenges

- hacking
- stigma of illegal nature
- government opposition
- acceptance
- ways to enable widespread use (sms transactions)

What lies ahead

- alternative cryptocurrencies, reduce dependence

Research questions

- size of bitcoin remittances
- use of sms transactions
- size of bitcoin donations

References

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system." *Consulted* 1 (2012): 28.

Ron, Dorit, and Adi Shamir. 2013. "Quantitative analysis of the full bitcoin transaction graph." In *Financial Cryptography and Data Security,* 6–24. Springer.