WHY BLOCKCHAIN MATTERS

Jason Guthrie – Head of Digital Asset Product and Head of Digital Assets
11 Feb 2020

The initial problem

While discussing the internet's potential for disruption in 1999, economist Milton Freidman posited:

"The one thing that's missing, but that will soon be developed, is a reliable e-cash: a method whereby on the internet you can transfer funds from A to B without A knowing B or B knowing A – the way in which I can take a $20 bill and hand it over to you…"

Since then, payments have undoubtedly become more digital. However, they have gone down a distinctly different path to the path envisaged by Freidman. What we have today is a system of 'trusted authorities,' where banks are the guardians of payment records. When you pay for something digitally, be that with a credit card in a store, via PayPal on a website, or by transferring money through a banking app, you're not actually sending money directly. Instead, you are initiating a relatively lengthy cascade of events involving a large number of intermediaries, which eventually results in your account being debited and the recipient's account being credited. You can find more details on this process here.

What this means is that, when it comes to digital payments, we are very much reliant on large credit institutions. Innovation is on their terms. Your ability to transact with a given party will depend on whether their bank is happy to talk to yours. Inclusion in a given market is driven by their criteria. They are the central point of failure; if your bank's systems are down you have limited options.

Digital payments challenges

So, how could a peer-to-peer digital payments system be developed?

As we start thinking about this, we'll be introducing two structural concepts; the Double Spending Problem and the Byzantine Generals Problem.

The double spend problem: In essence, this is ensuring that a given unit of money can only be spent once. If we think about cash, there is only a certain number of notes in existence and only one person can be in possession of a given note at a time so once it is spent it is gone. An obvious essential in any monetary system but a potentially difficult one to solve in a digital system if you think about the way other digital documents are transferred. When sending a document via e-mail what is received is actually copy of that document. The sender keeps the original. This is fine when sending a spreadsheet or a photo but not when sending money.

That's why banks – a trusted third party – have acted as a central authority up to now; If digital things can be copied infinitely then we need to rely on a trusted third party to keep track of how much everyone has.

So, to solve for this and create a peer-to-peer way of digitally transferring value, we need a way of all agreeing state of the world (i.e. who owns what) post each transaction without a central authority. This creates an issue of trust. A common analogy for this is the Byzantine General's Problem.

The Byzantine Generals problem[1]: this is a term that describes a situation where all participants in a system need to agree on a strategy in order to avoid catastrophic failure of the system, however, some participants are unreliable or malicious.

In the context of an electronic payments system, in order for the system to function without a central trusted authority, all participants need to have faith in the integrity of the system. When you have millions of participants who don't know each other wanting to transfer money, there is an enormous issue of trust that is difficult to overcome.

Bringing these two concepts together, what is needed is a technology that enables people to send value electronically to a third party without needing to know that third party, while ensuring that there's a permanent record of the transaction. If everyone in the system agrees that the transfer is valid and keeps a record of all transactions, participants cannot act fraudulently and no trusted third party is required, meaning the double-spending problem is resolved.

Blockchain: The technology of trustless record keeping

This brings us to blockchain. In 2008, Satoshi Nakamoto's paper, 'Bitcoin: A Peer-to-Peer Electronic Cash System,' proposed an e-cash system whereby 'trustless' peer-to-peer transfers could be made without the need for a trusted central authority to ensure there was no double spending. Shortly after, Bitcoin – the world's first cryptocurrency – was born.

Ultimately, it's the blockchain technology at the heart of Bitcoin that has allowed us to solve the inherent problems in electronic peer-to-peer transfers. And thanks to the open source nature of the Bitcoin protocol, the use of blockchain technology has extended well beyond the original cryptocurrency. Not only have many other digital currencies with innovative features been developed, but the technology has also been used in a broad variety of applications including:

- Register of shares
- Issuance of bonds
- Shareholder voting
- Land registers & title transfer
- Cross border transfers
- Digital Identity
- AML/KYC processes
- Peer-to-peer lending
- Securitisation
- Distributed peer-to-peer file sharing
- Transportation and fleet management
- Food traceability

- Supply chain

Why record keeping matters

At its core, blockchain technology is the technology of secure, trustless record keeping. It might not be as exciting as the 10x returns people typically like to talk about in the cryptocurrency space but this is the concept that has the potential to be truly disruptive.

When thinking about the applications of blockchain technology, the impact will likely be seen in three areas:

1. Removal of intermediaries

Many of the areas to which people are trying to apply blockchain Technology are often very expensive owing to the number of intermediaries that are involved in the system. Financial services are a prime example of this. Even for transactions that are relatively small, say $5 charge for using a card overseas or the 0.2% a credit card company charges a merchant, the institution responsible here make billions of dollars a year which could be returned to the end users of the system.

2. Efficiencies

Some assets are just very inefficient today. Anyone who has bought a house or transferred money to another country knows this. Blockchain technology is being used to put in place the rails to make the registration and transfer of many assets simpler, faster and cheaper.

3. Financial inclusion

Any services are limited by the size and available information. If we think about a company raising capital via an Initial Public Offering (IPO) they need to be of a certain size for banks to look at them. We also see many people in developing parts of the work without access to basic banking services as a result of difficulties in identifying them. Blockchain has the potential to lower the costs and improve data availability to lower the barriers to entry in various parts of the global financial system.

How to think about this going forward

There exists a lot of noise around this topic with the idea of blockchain being conflated with that of Bitcoin. The way Bitcoin uses the concept, and the community that has grown around it is interesting in its own right, but this is not the whole story of blockchain; Bitcoin was the original source of blockchain and is still the most visible application of the technology but there have been countless interactions and implementation of the concept since its launch. Some designed to challenge it as “the” cryptocurrency, some that could sit alongside it and many more still that have nothing to do with currencies or payment systems.

Regardless of people’s initial reactions or opinions on Bitcoin, when you take a step back from the details of a given use of blockchain, people pretty much universally agree that the concept of a trustless, peer-to-peer network of immutable record keeping has the potential for huge disruption. This technology has the capacity to increase the efficiency of human cooperation and unlock human capital to be deployed against humanities next great endeavour. When you think about it in this context, all blockchain based initiatives warrant a deeper consideration…

Source

[1] A full explanation of the Byzantine Generals problem can be found here: https://en.wikipedia.org/wiki/Byzantine_fault

Related products

+ WisdomTree Bitcoin

View the online version of this article here.

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.