The IOTA Distributed Ledger

A Massively Scalable Replacement for The Blockchain

Problems with the current paradigm

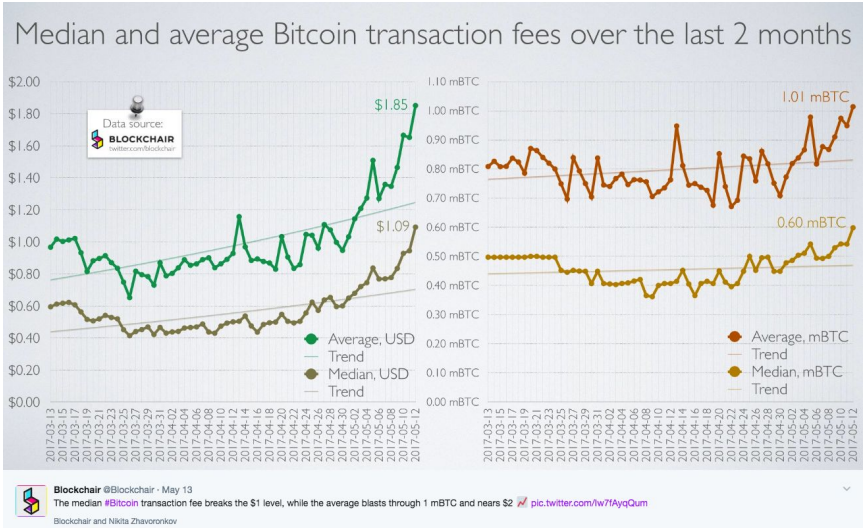
Distributed ledger technology (DLT) has gained popularity over the last few years, and is often touted as the magic bullet to all our data woes. But when we strip away the hype, there are a serious issues that plague the majority of DLTs, as they rely on blockchains. This is true of both Bitcoin and the increasingly popular Ethereum.

Despite the numerous strategies being attempted (such as increasing block size, fast payment channels, Segregated Witness, Proof-of-Stake etc), the fundamental problem is that these technologies depend on “miners”, entities who process all the transactions, and on an ever-increasing block of all the transactions (currently over 115 GB for Bitcoin), which must be stored by all miners.

This will cause 3 major issues that will affect the future usability and reliability of the system.

1. **Speed of transactions**
   Bitcoin has a theoretical maximum rate of 7 transactions / sec across the whole world, with Ethereum slightly better at 20 / second. In reality we are seeing speeds of under 5 / second in both. And remember that is all transactions in the world. There are currently over 140,000 pending transactions across the world on the Bitcoin blockchain (https://blockchain.info/).
   This is not scalable.

2. **Fees**
   Miners are required to process the transactions, and these miners must be paid. With increased use of the blockchain, the miners’ fees have increased significantly. Currently the average fee per transaction is $1.85 (blockchair.com) with an all time high close to $10. For one transaction.



Ethereum's fees are lower but also rising. Currently the median fee is over $0.06, with an all time high of $3.13 (http://ethgasstation.info/). Executing smart contracts also requires fees, usually double that of a transaction, for very simple contracts.
Again, this is not scalable.

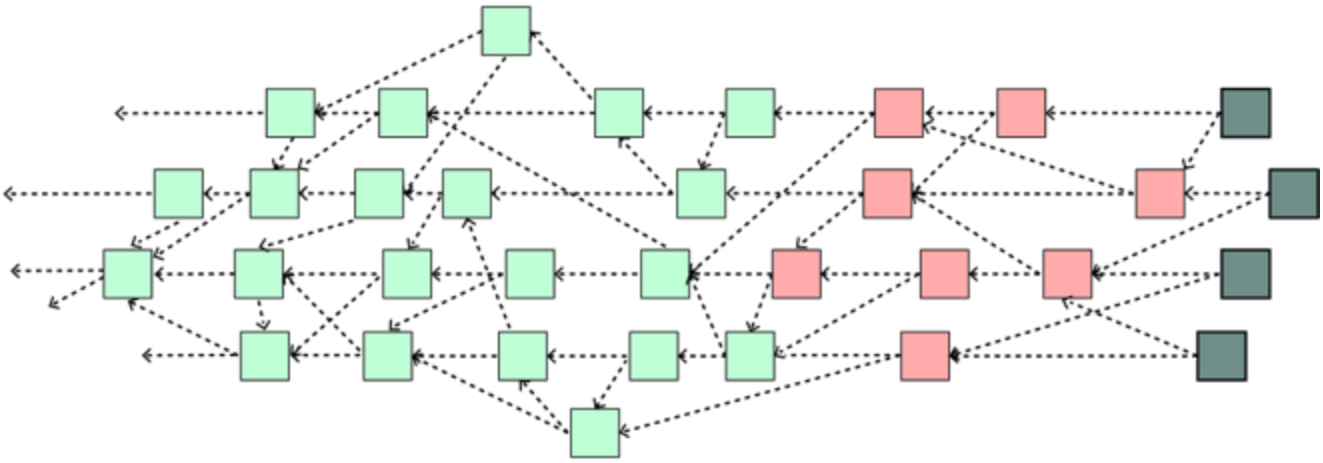
3. **Immutability and decentralisation**
   A DLT network is susceptible to attack when 51% of the mining power is controlled. Some say that 33-34% is sufficient (https://bitcoin.stackexchange.com/questions/38273/have-bitcoin-developers-applied-the-solution-for-selfish-miner-attack). The current Bitcoin blockchain is controlled by 5 main mining pools, a large proportion of which are in China. Should there be collusion between some of the mining pools, the integrity of the network is at risk. All blockchains are susceptible to this attack, as the high computational needs mean that miners tend to join pools, resulting in increased centralisation of transaction processing.

   One way that groups have tried to overcoming this issue is to use private (permissioned) ledgers, limiting the miners to people that can be trusted. However this means that even fewer transaction processors are involved, and therefore less need to be compromised to affect the integrity of the system.

The proposed use cases for distributed ledgers are limited by the transaction speeds and costs. However, were these limitations not present, we could begin to think about securing data at a massive scale - essentially a way to verify the integrity of all data. This is what IOTA aims to achieve.

Why is IOTA different?

IOTA foregoes the blockchain in favour of a more scalable architecture known as a Directed Acyclic Graph (DAG) - aka The IOTA Tangle:



In this architecture, there are no block or chains, and no reliance on miners. Instead the validation of transactions is performed by **every** participant in the network (ie true decentralisation) - each time a participant tries to perform a transaction, they must validate 2 prior transactions. After multiple rounds of validation, a transaction is deemed to have been accepted.

During each transaction, a small amount of proof-of-work must be completed (similar to the HashCash system) - this is much less onerous than the proof-of-work performed in blockchains, and acts only to prevent bad actors from taking over the network. Transactions are also signed with the Winternitz signature, a quantum-secure signature scheme.

This approach has the following benefits:

1) **Increased speed of transactions.** We have currently achieved transaction rates of 182 transactions / second with 250 participants. But the transaction rate grows with increasing participants (similar to the BitTorrent protocol), and high level stress tests are currently being performed with corporate and academic partners. We expect to demonstrate rates of over 1000 transactions / second soon.
2) **No fees**, as there is no requirement to pay miners.
3) **Increased security.** It would be incredibly difficult to control of 34% of all participants, in order to take over the network. Also the Winternitz signature is believed to be secure against attack from even quantum computers (https://eprint.iacr.org/2011/191.pdf).

Due to this unique architecture, we actively encourage people to transact on the network as this helps to validate other transactions. These transactions have no cost, and often may not involve transfer of value - they can instead be used to store data. This opens the door to a plethora of new use cases for the IOTA ledger, specifically in data sharing and provenance.
NB It is possible to set up private (permissioned) Tangles, but this may miss out on the transaction processing power of the main Tangle. However if there are a sufficient number of participants in the private Tangle, this may be seen as a feasible and desirable option in some circumstances.