

BLOCKCHAIN HAS NOT YET FOUND ITS PROBLEM

First View: Rapid analysis of breaking news, providing perspective

THE FACTS

Airlines, like many other enterprises, are currently subject to extensive marketing on behalf of blockchain technology providers. Lufthansa Group has joined SAP in creating an “Aviation Blockchain Challenge” which announced its first winners last month. The month before, Air France/KLM announced a relationship with Winding Tree “to develop Blockchain technology in the travel industry.”

THE ANALYSIS

The current expectations of blockchain resemble other technology booms in the past and perhaps provide an illustration of Amara’s Law which states that

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run”.

This has been expanded to create Gartner’s well-known hype cycle in which blockchain technologies are now firmly sitting somewhere between the Peak of Inflated Expectations and the Trough of Disillusionment. The question is whether blockchain will prove to be a dead-end development that never delivers on the hype or in the more optimistic scenarios it proceeds through the other phases of the cycle to end up on the Plateau of Productivity.

In the eyes of most casual observers blockchain is synonymous with cryptocurrencies such as Bitcoin. The speculation in Bitcoin that has seen its value peak at over \$20,000 before falling back to the current value of under \$4,000 at time of writing, while using as much electricity as a medium sized country, has ensured that Bitcoin and its miners remain in the news. However, it is important to separate blockchain technology from Bitcoin and other cryptocurrencies. Whether Bitcoin ever becomes an everyday medium of exchange for transactions such as buying airline tickets is a subject for another day. The immediate interest is in whether the underlying technology will find applications in which its unique attributes offer advantages that are not readily available by the application of other, perhaps more mature, technologies.

At its heart Blockchain is a distributed ledger in which transactions are recorded in blocks that are written in multiple locations or nodes. Each new block that is added to the chain



contains a cryptographic hash¹ of the previous block and is propagated across the many nodes that make up the network. The effect of this is that it is impossible to retrospectively alter any information that has been written to the chain without also changing every subsequent block in every location. In effect information written to the blockchain is permanent and unalterable. Also, the history of every transaction and every relationship mediated via the blockchain is readily available to every participant in the network. The nature of the blockchain is often described as dispensing with the need for trusted systems since every user can see everything that happens.

Although not strictly part of blockchain the concept of smart contracts is very much part of the surrounding hype. A smart contract is essentially an algorithm agreed between two or more parties that defines automatic responses to a set of inputs. Once agreed it is recorded in the blockchain where it is available to be invoked when the input conditions are met. For example, a smart contract might be set up between a power company and an industrial user. Every time the energy used crossed a threshold, software belonging to the customer could refer to the smart contract and trigger a payment. There would be no need to raise invoices or payment advice and the contract could include provisions such as discounts for off-peak consumption to be calculated automatically.

Like many previous innovations in technology smart contracts have been invested with exaggerated value by those looking to promote them. A smart contract is a piece of software that is designed to execute when certain conditions are met, without any further intervention. However, like any piece of software, it is not guaranteed to be free from defects and therefore to execute 100% correctly at all times. This should concern anyone who has ever written or used software. How can errors be dealt with in a piece of software that is guaranteed to execute? If it is possible to deal with them - i.e. prevent or significantly alter the outcome of execution - then this undermines the fundamental premise of guaranteed and automatic execution.

Even if it is possible to achieve a perfect smart contract, processes remain vulnerable to malicious manipulation of the conditions. It would be entirely possible to fake the inputs or conditions to either trigger or prevent execution of the smart contract. The integrity of supposedly “trustless” systems based on the blockchain still require the maintenance of trusted systems to manage inputs. Like every other software innovation smart contracts need to be properly understood and implemented with recognition of their strengths and limitations.

¹ This is a unique value calculated mathematically from the data in the block. Any change to the data would make the stored hash invalid, thus immediately alerting network participants to the change.

The many companies and individuals currently touting blockchain solutions to the airline industry are typically offering some combination of secure and indelible recording of transactions and smart contracts to streamline a business function.

In T2RL's opinion, none of the proposals for the travel industry has yet demonstrated that blockchain solutions offer a meaningful advantage over implementations based on conventional database technology. The reasons for this are largely twofold. Some proposals have simply not been thought through while others are hitting fundamental limitations of blockchain technology.

In a long and thoughtful blog post² a year ago, Kai Stinchcombe, CEO of True Link Financial LLC identified some of the many problems with trying to apply blockchain to the financial services industry. In his conclusion he said

"In conversations with bitcoin entrepreneurs and investors and consultants, there was often a lack of knowledge or even interest in how the jobs were being done today or what the value to the end user was."

This is a perfect description of many of the attempted entrants to the airline industry, including some that have gained traction with senior management in certain airlines. The fact is that the airline business is complex and much of the complexity is there for a good reason. Simply making sweeping assumptions about existing processes being stupid or outdated and needing to be swept away is a sure recipe for failure.

Ultimately however if an entrepreneur has an idea with real value it will be possible to work with industry experts to refine it to the point where it is actually viable. If by that point it retains enough of its claimed benefits it may be adopted and eventually reach the Plateau of Productivity.

The more fundamental problem with blockchain is that unlike other technologies there are no economies of scale with a blockchain solution. In fact – and by design, every incremental transaction processed is more expensive than the ones preceding it. This is due to the design of the blockchain in which every piece of information is retained at every node in the network and must be propagated through the network every time a block is written. This means that the resource requirements to perform each transaction increase over time. While this may be partially offset by the continued operation of Moore's Law, the transaction volume of most airline requirements means that economic viability of a blockchain solution will be a receding target.

There is also a significant issue of latency inherent in the design of the blockchain. A well-known finding in computer science known as Brewster's Theorem or the CAP Theorem

² <https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100>



states that it is impossible for a distributed data store to satisfy all three of the following guarantees:

Consistency: Every read receives the most recent write

Availability: Every request receives a response – without the guarantee that it contains the most recent write

Partition tolerance: The system continues to operate despite network failures between its nodes

The practical consequence of the CAP theorem is that a network that needs high integrity can only achieve this by inserting a significant delay between writing to a block and making that result available to be read. Typically, this is done by a rule that says data is not available to be read until some arbitrary number of blocks has been written after the one that contains it. With blocks being added at intervals measured in minutes rather than milliseconds this would rule out blockchain for many high throughput applications.

THE SPECULATION

The discussion above would seem to suggest that T2RL is highly sceptical about the application of blockchain to most airline requirements. This is certainly true in the short term. A combination of naivety on the part of developers and the inherent limitations of the blockchain architecture means that we do not envisage significant value being generated over the next few years.

However, it is important to avoid the opposite pitfall to that being encountered by the blockchain evangelists today. The second clause of Amara's Law may apply. There may be applications that will be well served by a derivative of the technologies being developed today and it is important to maintain a balanced view. In doing that the key requirement is to consider applications for which the inherent characteristics of blockchain solutions may be valuable. This quickly rules out the high-volume, low-latency transactions around air shopping. On the other hand, it suggests that lower volume functions, especially those involving multiple external partners may benefit from the indelible ledger and algorithmic contracts made available. An example might be an airline's vacation packages offering in which flights are combined with hotel, cruise and ground packages from third parties. In today's world there is a real challenge involved in ensuring that partner inventory remains available when it is needed and at the price agreed. A distributed ledger with smart contracts has the potential to solve this problem.

Whether the airlines putting money into blockchain today will ever see a direct return on their investment is very doubtful indeed but it is just possible that the experience gained today may have some value in the next generation of technology – or the one after that.





T2RL is an independent research and consulting company that specialises in the market place for airline IT systems. Based on data gathered and analysed since the year 2000 it has defined and tracked classifications of airlines and their IT providers. Its research is used by airlines to enable them to make informed choices of systems and vendors and by the vendors to help them develop products that best meet the current and future needs of the airline industry. For further information, visit our website at www.t2rl.com.

