AFRIDI & ANGELL
LEGAL CONSULTANTS

Since 1975

inBrief

Blockchain: Hype vs Reality

By James Bowden and Abdus Samad | 23 April 2018

Over the past 1-2 years, a great deal of information concerning the revolutionary technology that is "blockchain" has been published on many business, legal and technology news sources, and innumerable self-proclaimed authorities on the subject have emerged to contribute articles and presentations (ourselves among them). Sometimes the information offered is insightful and helpful, but far too often the message is a surface level parroting of various platitudes that have become associated with all things blockchain without more meaningful explanation, leaving the audience with no useful information and only a vague sense that blockchain is important somehow. Using words such as "*transformational*" and "*revolutionary*", industry leaders have described this technology as the next major step in human technological progress. We certainly agree that it appears to be important; however, we advise approaching the subject with the normal healthy skepticism with which you would approach any other subject matter which you might not fully understand. This can be difficult with so many blockchain evangelists dominating the media, and too few people pointing out its limitations.

In this briefing, we explore some of the most common claims that are made about blockchain technology in an effort to curb what strikes us as often irrational enthusiasm and to encourage critical thought.

Brief Summary of Blockchain

Blockchain can best be described as a ledger system that, rather than recording and storing information on a central system or server, is stored and maintained on multiple servers that are connected over a network using a blockchain application. Hence the term "distributed ledger". Every time there is new information added to the ledger (i.e., any transaction occurring on that particular blockchain network), the new entry is verified by a majority of the network nodes (members of that blockchain network) with reference to past transactions recorded on that

The Authors

James Bowden
Partner
jbowden@afridi-angell.com
Tel: +971 4 330 3900

James heads the data privacy and cyber security practice at Afridi & Angell. He advises companies in the TMT sector on industry specific regulatory compliance as well as on general corporate and commercial matters. Prior to joining Afridi & Angell, James gained in-depth technology outsourcing experience while working as in-house counsel with one of Canada's leading technology companies. He is a member of the Ontario Bar.

Abdus Samad
Associate
asamad@afridi-angell.com
Tel: +971 4 330 3900

Abdus advises foreign and local clients on general corporate, commercial and other matters related to the conduct of business in the region including corporate investments, restructuring, setting up companies and joint ventures in the UAE, and the acquisition and sale of business. Abdus has also been involved in banking and finance transactions, and advises clients on banking related products and services.

blockchain, and periodically groups of entries at a time are consolidated into what is referred to as a "block". Block after block of data entries are created and are linked in chronological order, and this is the "chain" or "blocks". The creation of a block, and the linking of each block to the last and the next in the chain, are simply cryptographic events carried out by the software and in total can be thought of as a process of protecting the entries through encryption. Do not visualize blocks and chains; just understand that the data is being powerfully encrypted to render it very difficult to retroactively alter. It therefore seems to us that, in the simplest of terms, blockchain can be regarded as a new method of storing and sharing information electronically.

We will now set out a series of claims or statements that are frequently made about blockchain and will give our views on each.

Blockchain takes [X] process and makes it transparent (like a manufacturing process plus shipping and distribution of the end-product).

This often-cited claim envisages a scenario where all interested parties (such as buyer, seller, manufacturer, shipping line, banks) are members of a particular blockchain application which would record all steps in the lifecycle of a given transaction, from placement of an order to different phases of raw material acquisition and manufacturing, packaging, shipping, delivery and payment. The transparency claim is based on the fact that everyone on that particular blockchain network would have access to all of the entries on that blockchain, and assumes that entries would be made throughout the process in question, providing a running real time update. Users would then be able to see the provenance of all materials used in a manufacturing process, how the process is going at any given time, and where the goods are. This claim is perfectly laudable, but it is far from revolutionary. This is essentially an observation that data can be shared electronically, and that being a member of a blockchain network is one way to do that. Email is another way. Posting updates to any forum accessible to the relevant parties is another. Proponents will cite the improved reliability of the information when it is made available through a blockchain application because it cannot be "hacked", and therefore reduced fraud. This is positive, but the incremental nature of the benefit should not be lost amidst claims that attempt to credit blockchain technology with enabling electronic communication.

Putting information relating to a transaction (such as a shipment of goods) onto a blockchain prevents fraud.

While it may be accurate to say that putting information relating to a transaction onto a blockchain reduces the costs and time delay in multi-party business activities, the mere act of recording and sharing information in blockchain format clearly cannot prevent underlying fraud in a commercial transaction. The source of the information being entered must be understood (human or machine? reliable?). It is important to understand that a blockchain verification process does not guarantee that any entry will be factually correct. Indeed, it has nothing to do with that. Blockchain software only verifies that the transaction was entered by a valid user (or someone with the password) and that it is a logical possibility when considering the past transactions (e.g., you cannot create fake goods where none existed on the blockchain, but you can say they are complete when they are not). To take an example, imagine a commercial transaction concerning the sale of ballpoint pens. The purchaser wishes to purchase 5,000 black ball point pens and the seller offers to sell the purchaser 5,000 black ball point pens. Unknown to the purchaser, blue ballpoint pens are substantially cheaper to manufacture than black ones, and the seller could save a substantial amount of money by shipping blue pens rather than black pens. In the event that the seller chooses to ship blue pens instead of black pens, the fact that the underlying contract is stored and exchanged on a blockchain will not eliminate the ability of the seller to ship blue pens, should it decide to do so, and to enter confirmation on the blockchain that the order is filled and shipped, just as the seller could have done by sending an email to that effect.

We have no doubt that blockchain can indeed help with the reduction of fraud in commercial transactions, especially with the growing integration of sensors and devices which automate reporting, removing the factors of human error or deceit to some extent. The creation of an immutable audit trail on the blockchain should help deter fraud as well. However, it is important to place things in context and to appreciate that as

things stand at present, you should stress test claims of fraud prevention by asking questions about the source of the information that will be added to the blockchain and understanding whether (or rather how easily) it can be manipulated.

Blockchain removes the need for "trust" in a transaction because all transactions get verified by the network (put another way, blockchain disrupts the disruptors by removing the need for trusted intermediaries like Air BnB or Uber).

It is often said that by placing a contract on a blockchain (i.e., by creating a "smart contract"), parties to a contract eliminate counterparty risk and also eliminate the need for "trust" in a commercial transaction, and by extension trusted third parties like banks, aggregators, brokers, escrow agents, etc. This is, in our view, perhaps the boldest claim that is asserted frequently, with the least compelling evidence in support. The issue relates to two main things: 1) information verification, and 2) smart contracts.

Information verification: the argument is something like this. Companies like Air BnB or Uber are aggregators and middle men that help connect individual users to individual service providers, and their role is essentially one of quality control and oversight of behaviour on their service, and also to accept a measure of responsibility for the product being provided to users. If those services were blockchain-based, listings would be verified by the network and would be fully transparent, so there would be no need for a company to fill the role of supervisor or quality controller. With reliable information at their fingertips, users could rely on the technology instead of an intermediary. Our concern with this proposition again relates to the quality of the source of the information being entered. Simply because the information is verified by the network as having been validly entered does not mean the information is accurate. Nothing would prevent an Air BnB user from posting a misleading description or photographs of a house. At least with an administrator involved there is some level of accountability and a party that actively takes an interest in verifying the quality of listings and organizing them. Absent this, you would presumably rely on comments and feedback against the listing and with those, just as with the listing, you would have no way of knowing whether they were genuine. It may well be that, from a user experience point of view, we would all very much prefer to retain a responsible/trusted third party to organize and police the service. Most users would probably not find the prospect of reviewing entries on a blockchain very appealing, even if it meant they could extract reliable information from it.

Smart contracts: A smart contract is said to be beneficial because it "executes itself" or "executes automatically", without the need for human intervention, approval or action. For most types of contract, this is simply not true. While it is correct to say that a smart contract contains a certain set of rules to deal with a set of variables (e.g. if Y happens than X must happen), such contracts are not (yet) in a position where they can eliminate counterparty risk in any but the most simplistic and mechanical of transactions. To take a common example, assume that a truck full of fruit is ordered and is being transported from Dubai to Abu Dhabi. The parties enter into a smart contract stipulating that so long as the temperature in the truck has not fallen outside of the permitted range (e.g., -1 to 2) for more than 3 minutes throughout the journey, payment for the fruit will automatically be transferred to the seller. Such an example assumes several things. First, it assumes that the technology on the truck will give reliable temperature readings which are beyond dispute and will transmit them (perfectly plausible). GPS readings will also be sent automatically to confirm when the truck leaves and arrives (also perfectly plausible). These two objective pieces of information are "internet of things" benefits, which are entirely unrelated to blockchain technology. Since that data is online, it can be made available automatically to the blockchain network on which the smart contract resides (i.e., the smart contract will know the temperature and location of the truck, so this is good). However, the example also assumes that the seller has loaded the required type and quality of fruit. This requires human verification, and the smart contract cannot know this unless someone inputs that confirmation to the blockchain network. It also assumes the right quantity of fruit has been loaded. The truck could be weighed, but the weight could be comprised of anything, not necessarily the expected fruit. The factors that a smart contract must rely upon, but which it cannot know without human input, are called "external dependencies", and as soon as you

have even one external dependency, you lose the theoretical benefit of self-execution. This is one example of one type of limitation that affects the viability/usefulness of smart contracts in a conventional commercial world, but there are several others, which we will not elaborate on due to space constraints in this article. Our point is not that smart contracts have no use (they surely do), but rather that their utility is often overstated and that it is important to think critically about how any given smart contract operates.

If it's on a blockchain, it's impossible to hack.

The security and integrity of a blockchain relies on the underlying encryption and on the fact that a blockchain is a distributed ledger. Each block in a blockchain builds upon the block immediately prior to it, and a would-be hacker would not be able to tamper with the last block without also tampering with all of the previous blocks and also ensuring that each copy of the ledger maintained on at least a majority of the nodes on any given blockchain is uniformly tampered with simultaneously. We have to take the truth of that statement at face value, although as with so many of the accepted benefits of blockchain, we as legal advisors cannot claim to have independently verified that this is accurate from a technical/coding/encryption perspective. Assuming it is accurate, then it is true that in order for a hacker to undertake such an exercise, he or she would require an enormous amount of computing power. It is also true that such computing power is probably not mainstream at present. However, this may change as technology develops and blockchain gains prevalence. We have no reason to doubt the extreme difficulty of hacking data stored on a blockchain application.

You may ask yourself, what about all of the high profile bitcoin and ethereum hacks that have resulted in so many people having their cryptocurrencies stolen? These were not hacks of the underlying information on the blockchain, which in the case of cryptocurrencies records and tracks who owns and transfers how much of the cryptocurrency. Rather, they were hacks of the exchange or the user accounts, which can be thought of as access points to the blockchain such that instructions to transfer appeared to be from a legitimate source. It is comparable to stealing someone's gmail password: as far as gmail is concerned the activity appears legitimate, and gmail was not hacked, only your device was hacked.

The takeaway to bear in mind is that while blockchain-style encryption is probably extremely difficult to hack, access points remain vulnerable just as with any other application. If your credentials can be misappropriated or authorized users impersonated, information on a blockchain is still vulnerable.

As an individual using a blockchain-based application, what will you see or do differently from today?

Looking at the actual entries in a blockchain application is not very user friendly, and it is not intended to be read and interacted with by humans. It is back-end infrastructure, upon which user-friendly interfaces are built, just like website interfaces that sit on top of underlying code. The look and feel of interacting with a blockchain application should be no different than the applications and websites we see today. The revolutionary nature of the technology is attributable to its underlying merits around security and transparency, and what will change is how the information is recorded and shared, but it should not require any special skills or learning simply to interact with it as a user. On the other hand, if you wish to learn to read the code that drives a smart contract, this will require learning to read code and will not be intuitive with that skill set.

We are optimistic about the benefits that blockchain technology and its uses can and certainly will bring, and we hope that the above is taken in the manner intended, which is only to advise that enthusiasm around all things blockchain be tempered by healthy skepticism and thorough understanding. ■

Afridi & Angell

Founded in 1975, Afridi & Angell is a full-service UAE law firm in its fifth decade at the forefront of the legal community. From the beginning, our hallmarks have been a commitment to quality, unsurpassed knowledge of the law and the legal environment, and crafting of innovative business solutions. Licensed in the three largest Emirates of Abu Dhabi, Dubai and Sharjah as well as the Dubai International Financial Centre, our practice areas include banking and finance; corporate and commercial law; arbitration and litigation; construction; real estate; infrastructure projects; energy; project finance; maritime (wet and dry); and employment. We advise local, regional and global clients ranging in size and sophistication from start-ups, sole proprietorships, family-owned businesses, entrepreneurs and investors to some of the world's largest public and private companies, governments and quasi-government institutions. We attract and retain clients with our dedication to practical guidance focused on their business needs supported by decades of experience here in our home jurisdiction, the UAE.

Afridi & Angell is the exclusive member firm in the UAE of top legal networks and associations, most notably Lex Mundi, the world's leading network of independent law firms, and World Services Group.