Editorial

Will blockchain technology revolutionize excipient supply chain management?

Shireesh Apte[a*], Nikolai Petrovsky[b]

[a]Editorial Board, Journal of Excipients and Food Chemicals
[b]Department of Endocrinology, Flinders University, Bedford Park, Adelaide, Australia 5042

KEY WORDS: Blockchain, excipient supply chain, excipient, bitcoin, supply chain, pharmaceutical

A 'blockchain' is a distributed public consensus system that maintains an immutable record of transactions on the web, incapable of being falsified after the event. The cryptography behind the protocol is based on asymmetric encryption modulo mathematics where the 'key' for encrypting a message or transaction is different from the 'key' to decrypt it. The algorithm accomplishes this by splitting the key into a private and a public key that are mathematically linked trapdoor functions. By calculating modulus functions of mutually known starting numbers, only the sender and recipient can encrypt and decrypt messages using their own different private keys, while the transaction itself can be verified publicly by using the 'public key'. Since it requires no 'central authority' as a 'book-keeper', transactions are faster depending upon the number of nodes that mine the data at any particular point in time. The usual incentive to verify (mine) the blockchain is the dispensing of bitcoin. However, as the supply of this algorithmically designed anti-inflationary crypto-currency dwindles, that incentive could be a transaction fee or linked to remuneration in goods and services.

What does all this mean to pharmaceutical manufacturers in simple terms? The blockchain is a simple way of passing information, which could include embedded financial transactions, from party A to B to C to…Z in a fully automated and safe manner without the need for intermediaries, whereby the final receiving party Z has direct access to the complete and non-falsifiable web-based transactional record tracing all the way back to originating party A. The first party to a transaction initiates the process by creating a block. This block is verified by multiple computers distributed around the net. The verified block then becomes the starting point for a chain of blocks as the contents are passed from party to party which is stored across the net in multiple copies thereby creating an indestructible single unique record including its whole transactional history. This effectively creates an accounting ledger that can never later be changed or falsified given that this could only be done by changing or falsifying every single copy of the ledger distributed across the net, which would be effectively impossible. In effect, copies of the blockchain are stored at multiple places in the

*Corresponding author: 5204 Coventry Court, Colleyville, TX 76034, Tel: 817 501 2984, e-mail: shireeshpapte@msn.com

cloud, thereby providing assurance that even if one storage site was knocked out by a catastrophe; sufficient copies would remain such that the block chain would not be lost. This exploits the same feature of the web that underpinned its creation, namely the idea that whole areas of the network could be wiped out for example by nuclear war and yet the information stored on the network would be preserved.

Blockchain advocates claim transparency, speed, accessibility and non-falsifiability as the cornerstones of this new paradigm. Blockchain technology should make it much more difficult, if not impossible, for illicit or counterfeit products, for example, adultered or non compliant excipients, or goods whose processing is environmentally detrimental to enter legitimate supply chains. It would enable end users to verify exactly how, where and by whom the product they intend to purchase has been assembled and made, thereby denying a market for illegal and counterfeit products.

While the veracity of transactional records (as distinct from actual transpired events), the chain of custody is unalterable, this fact, in and of itself, is no indication that an excipient has remained unaltered in transit or at the point of source. Indeed, just as in current supply chain verification methods, where rogue collusion exists within the supply chain there can be no guarantee that what is transacted in the blockchain (such as the attributes of a certificate of analysis) is actually congruent with the chemical make up of the excipient or material. Similarly, a chain of custody transaction records is no guarantee of the actual physical whereabouts of the material en route from supplier to end-user. Just because a transacted record is computerized and 'blockchained' does not necessarily imply that its physical world counterpart material of commerce has not been tampered with; all it implies is that the transaction record cannot, and has not, been tampered with. Of course, block chain veracity is reliant on appropriate audit processes to verify each transactional record to ensure it is accurate at the time it is entered into the blockchain. Providing this is done, it is not possible for the transactional ledger to be subsequently adulterated to hide, or change, a particular step to, for example, change the real source of a reagent, certificate or process. This is an important advance as it means that any falsification of the material source has to be done prospectively in real time, which is a much harder challenge, than at any time retrospectively falsify a physical transactional record, where hard copy documents can be simply substituted with new versions containing different facts

This is a very important advance in the authentication and validation of supply chains, but it is not able to, and was never intended to, replace traditional quality and auditing processes needed at each step of prospectively creating a transactional record. In fact, as each of these auditing steps are completed they too become part of the transactional record, so that someone at the end of the supply chain can verify that appropriate audits have been undertaken by appropriately credentialed authorities and can hereby 'trust' the whole transactional record.

Whether public or private, the possibility of 'miner' collusion (parties controlling mining servers performing verification of the transactional records on the web) obtaining > 50% of the network's hashing power could present a threat to the consensus protocol thereby allowing the miners themselves to enter illegitimate transactions into the block chain. These may range from over-invoicing, changing quality documentation, testing protocols and/or contracts, changing exclusivity, 'preferred supplier' or sub-contract clauses, changing shipping, distribution or repackaging logistics. However, this would require the miners to be colluding and working for a particular supplier, as the miners themselves just verify the record but do not have access to its contents. Paradoxically, such attacks are more probable in so-called private blockchains which may not require extensive 'proof of work' processing across multiple independent servers to achieve consensus. If transactions on the blockchain are contractually obligatory, then such attacks could prove disastrous for the end-user. In a sense this is no different to currency, which we rely upon for global commercial transactions accepting nevertheless it is not a perfect system and at any one time a give percentage of this currency will be counterfeit.

Blockchain technology provides a major advance for excipient supply chains, assisting in the delivery of unadulterated, source, process and transit verifiable excipients (or APIs and drug products), but does not alleviate the necessity for quality audits. As IPEC-Americas argues, there is no substitute for knowing and communicating with your supplier, random audits by certified bodies of the supplier and supply chain, and chemical testing to validate and authenticate a supply chain. The adoption of blockchain technology should make the process faster and make the transactional record more robust and reliable, however other rate-limiting steps of the excipient supply chain including transit and testing time will remain. In terms of pure speed, blockchain is suited to financial transactions where no physical goods change hands (such as financial instruments and derivatives, stocks, insurance, land-registry, taxation, medical records etc.) but this does not mean that it should be ignored in respect of the advantages it could offer in improving the excipient supply chain.