42 *Int. J. Blockchains and Cryptocurrencies, Vol. 1, No. 1, 2019*

Mathematical assessment of blocks acceptance in blockchain using Markov model

Riktesh Srivastava

Skyline University College,
Sharjah, UAE
Email: riktesh.srivastava@gmail.com

Abstract: Blockchain, introduced in bitcoin system is disrupting the way transactions are done in businesses via charging small transaction fees. It is observed that the acceptance of blocks in the blockchain is based on transaction value. Transmittals through blockchain are favoured due to low transaction cost and grander security. However, attempt of implementing blockchain to revolutionise business processes writhes from problem of waiting time for blocks. In this paper, the transaction-confirmation-time is appraised using queuing theory, where the approval rate of blocks in blockchain is concocted using Markov queue model. Four specific use cases of 1, 3, 6 and 60 confirmations are considered for practical purposes.

Keywords: blockchain; transaction-confirmation time; distributed consensus mechanism; Markov model; waiting time.

Reference to this paper should be made as follows: Srivastava, R. (2019) ‘Mathematical assessment of blocks acceptance in blockchain using Markov model’, *Int. J. Blockchains and Cryptocurrencies*, Vol. 1, No. 1, pp.42–53.

Biographical notes: Riktesh Srivastava holds a PhD in Electronics Engineering, Master’s in Electronics Engineering and management qualifications in Marketing Management and General Management from Indian Institute of Management, Ahmedabad (IIMA). Furthermore, he has also completed prestigious certifications on marketing analytics and electronic commerce from Wharton School, University of Pennsylvania, USA and NTU, Singapore, respectively. He has written three books (*OS*, *C++ Programming* and *RDBMS*) and published more than 50 papers in international journals and conferences. His areas of interest include machine learning, big data analytics, queuing theory and presently also indulged into studying theoretical concepts of blockchain technology as well. Currently, he is a faculty, School of Business, Skyline University College, Sharjah, UAE.

1 Introduction

There is no doubt that use of blockchain will disrupt businesses across all sectors (O’Sullivan, 2018). The fact that blockchain provides distributed and decentralised transactions – trust (Lin et al., 2017; Elsden et al., 2018) and transparency of information (Wüst and Gervais, 2017; Faour, 2018), makes it appealing for businesses. Initially, blockchain was virtual and public ledger system to record the transactions in a secure and transparent manner (Agrawal, 2018). Lately, blockchain is used by many businesses for various other purposes (Pepijn, 2017) as mentioned below:

- Walmart uses blockchain to record the contents of each package (Milano, 2018)
- Maersk adopted blockchain for documentation process as shared transaction (http://www.valtech.com, 2018)
- British airways uses blockchain to maintain data between destinations to avoid the conflicting information (Nash, 2018)

The advantages of blockchain finds its importance in almost each aspect of business, wherein every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared (Iansiti and Lakhani, 2017). If that happens, then, need of intermediaries will no longer be necessary, and businesses would freely transact and interact with one another through blockchain, with minimal friction. Though advantages of blockchain technology are immense, it still cannot be in the mainstream business due to scalability issues (Sherman, 2017; Martindale, 2018). With PayPal and Visa processing 1,667 and 450 transactions per second, while ethereum and bitcoin does 20 and four transactions per second respectively (Altcointoday.com, 2017), if we really want to use blockchain for various reasons, it would not be conceivable as of this moment due to slow transaction rate.

The slow transaction rate in blockchain is because of the consensus methodology adopted as necessity of inclusion of blocks in fork of blockchain. The current strategy is at least six consensuses for 1,000,000 or less and 60 otherwise.

The present paper proposes inclusion of Markov model of queue along with consensus mechanism for faster inclusion and transaction thereafter. Markov model deemed fit for the study as inclusion of block in the main fork of blockchain is independent of each other and solely depends on proposal of nonce by the miner to be verified by at least six other nodes.

Rest of the paper is divided as follows: Section 2 defines the decentralisation process in a blockchain with emphasis on distributed consensus mechanism and confirmation requirements for blockchain. Section 3 analyses the waiting time of transaction to be part of blockchain using Markov model and with identified number of confirmations. Section 4 evaluates the proposed model for ten blocks inclusion rate. Section 5 concludes the study with observations and future course of action.

2 Blockchain and decentralisation

There are deliberations about blockchain to be distributed and decentralised (Feld et al., 2018; Stifter et al., 2018) and the most novel method to build distributed and decentralised blockchain system is consensus mechanism (Baliga, 2017; Efanov and Roschin, 2018; Hull, 2017). The concept of consensus states automatic selection of next block to the blockchain with the following steps:

1 both smart contract and transaction gets broadcasted to all the nodes

2 each nodes collects either/both of them

3 [lottery race] a random node is selected to broadcast its block

4 other nodes accept the block if it includes valid contents

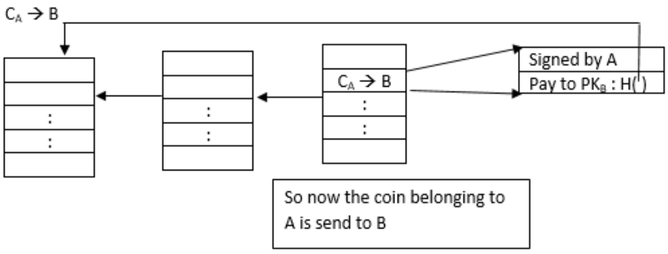
5 nodes express acceptance of the proposed block by including its hash in the next block they create.

2.1 Necessity of consensus mechanism

Although consensus mechanism slows down the inclusion of blocks, it is necessary part of blockchain and cannot be avoided.

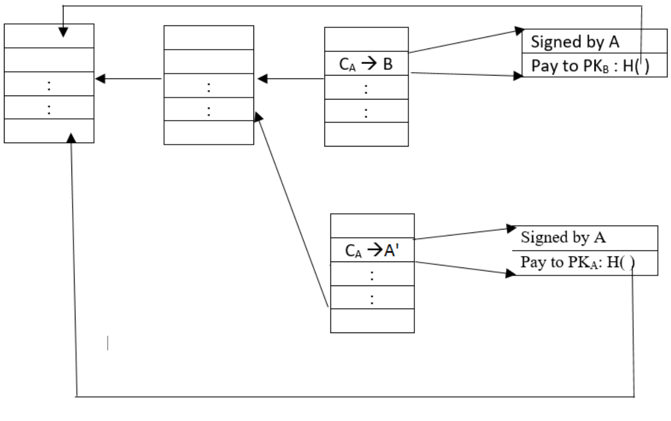
The scenario is elucidated in the following example, with A wants to get service from B, then A has to follow the conditions mentioned in smart contract, and payment is conducted in cryptocurrency. The actual transaction happens something as mentioned in Figure 1.

Figure 1 Transactions in blockchain



In the above-mentioned case (as mentioned in Figure 1), the proposed block is an honest node and, thus, accepted. However, there may be the scenario where instead of $C_A \rightarrow B$ transaction, A acts in a malicious manner and does $C_A \rightarrow A'$, as mentioned in Figure 2.

Figure 2 Malicious transaction in blockchain



In other words, $C_A \rightarrow A'$ indicates that A instead of paying to B has conducted the transaction to A′, which is another address controlled by A. This attack is called double spending attack, (Pérez-Solà et al., 2018; Karame et al., 2012) and technically, the transactions are valid in all aspects.

There are possibilities that next block proposes $C_A \rightarrow A'$ block instead of $C_A \rightarrow B$ node, followed by other set of nodes as mentioned in the Figure 3. Since, there is a rule of selection of longest blocks in a blockchain (Lewenberg et al., 2015), $C_A \rightarrow A'$ is a part of longest chain, double spending has succeeded over set of honest nodes.

Double spending attack is the most common type of attack that happens in blockchain (Karame et al., 2012). And if that happens, the customer starts using the services from merchant without even paying for it. The solution provided was to get minimum number of confirmations, as cited in Figure 4, before letting the customer using the services (de Leon et al., 2017; Gatteschi et al., 2018; Shi, 2016).

Figure 3 Malicious blocks selected being longest in chain

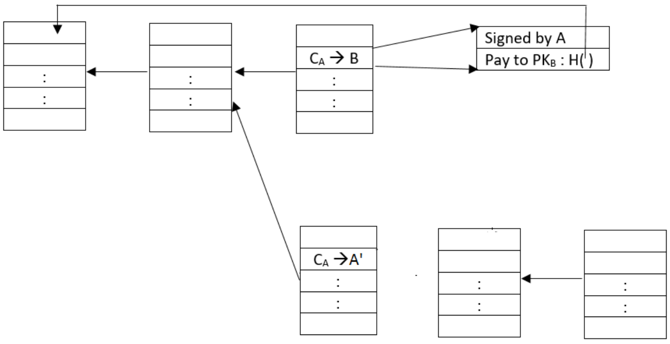
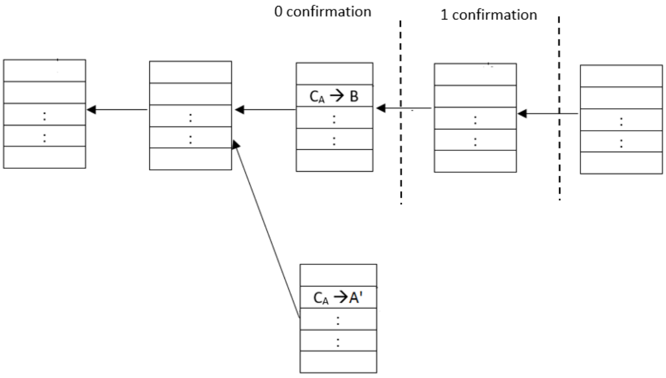


Figure 4 Confirmation rule in blockchain



Bitcoin (2017) proposed the following rule for blockchain confirmation, as stated in Table 1. The rule clearly indicates that number of confirmations is dependent on sum of transactions in a block. Once the block is created and the new transaction is confirmed and built-in that block, the transaction will have one confirmation. Around every ten minutes subsequently, a new block is generated and the transaction is reconfirmed by blockchain network (Miers et al., 2013; Jang and Lee, 2018). While some services are instant or only require one confirmation, many companies implementing blockchain requires more number of confirmations. Most common assumption is that if we get six confirmations (six blocks consensus), its considered to be valid transaction (Neumayer et al., 2018; Akcora et al., 2017).

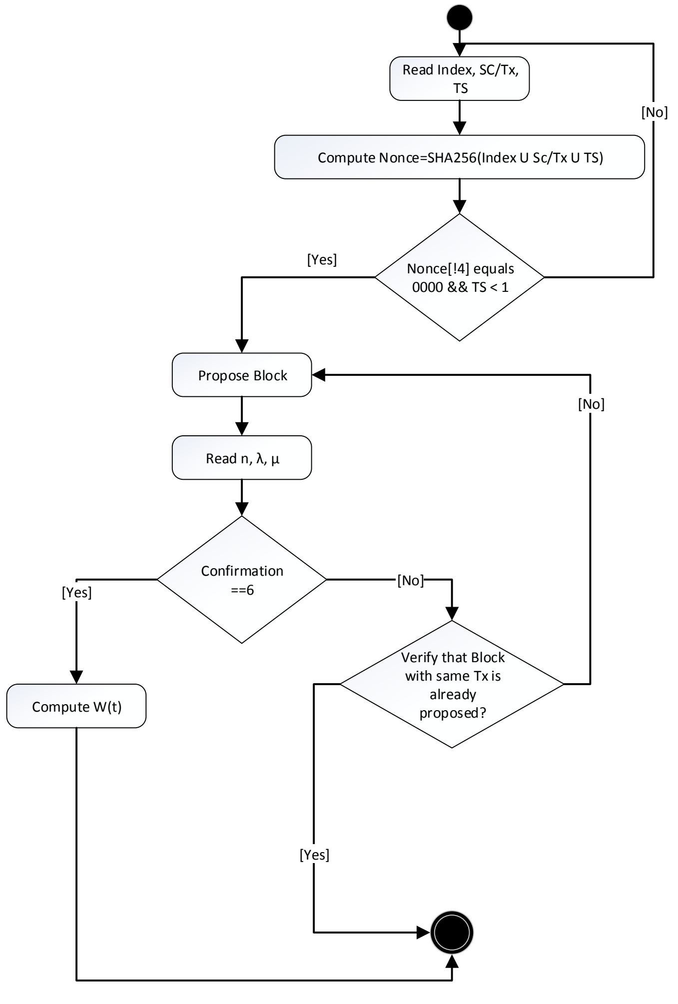
Table 1 Confirmations in blockchain

No. of confirmations required	*Transaction amount*
1	Sum(Tx) < 1,000
3	Sum(Tx) > 1,000, Sum(Tx) < 10,000
6	Sum(Tx) > 10,000, Sum(Tx) < 1,000,000
60	Sum(Tx) > 1,000,000

2.2 Execution of consensus mechanism

Figure 5 elaborates the execution of consensus mechanism, followed by snippet of Python code, used to conduct the experiment.

Figure 5 Process diagram for estimation of waiting time for each block after six confirmations



The Python code of inclusion of blocks in blockchain is given as under:

```
class blockchain:
def__init__(self):
self.chain = []
self.create_block(proof = 1, previous_hash = '0')
def create_block(self, proof, previous_hash):
block = {
'index': len(self.chain) + 1,
'timestamp': str(datetime.datetime.now()),
'proof': proof,
'previous_hash': previous_hash}
self.chain.append(block)
return block
def get_previous_block(self):
return self.chain[-1]
def proof_of_work(self, previous_proof):
new_proof = 1
check_proof = False
while check_proof is False:
hash_operation = hashlib.sha256(str(new_proof**2 -
previous_proof**2).encode()).hexdigest()
if hash_operation[:4] =='0000':
check_proof = True
else:
  new_proof += 1
  return new_proof
def hash(self, block):
encoded_block = json.dumps(block, sort_keys = True).encode()
return hashlib.sha256(encoded_block).hexdigest()
```

3 Analytical study of Markov model for blockchain

For estimation of n blocks arriving to get confirmation by miners, certain assumptions are to be made. This can be given as follows:

1. Δt is a very small time, in which only one block is processed. In case of blockchain, $\Delta t = 1$ second, as generation of previous_hash takes timestamp also.
2. The state of arrival of blocks for any miner is λ and after confirmation/non-confirmation, state of departure is μ.

Based on two assumptions, following four states are observed (Srivastava, 2013):

- probability of one block arrival = $\lambda.\Delta t$

- probability of no arrival of block = $1 - \lambda.\Delta t$
- probability of one departure (orphan block) = $\mu.\Delta t$
- probability of no departure (no orphan block) = $1 - \mu.\Delta t$

Now, consider that there are n blocks present at any time t.

Then probability of these blocks to be part of blockchain is $P_n(t)$.

If the time is increased from t to $t + \Delta t$, then there are following three possibilities:

$$P_n(t+\Delta t) = \begin{cases} P_n(t)(1-\lambda\Delta t)(1-\mu\Delta t) \\ \quad P_{n+1}(t)(\mu\Delta t) \\ \quad P_{n-1}(t)(\mu\Delta t) \end{cases} \tag{1}$$

Arranging the conditions in equation (1), we get

$$P_n(t+\Delta t) = P_n(t)(1-\mu.\Delta t)(1-\mu\Delta t) + P_{n-1}(t)\lambda\Delta t + P_{n+1}(t)\mu\Delta t \tag{2}$$

Or

$$\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = -\lambda P_n(t) - \mu P_n(t) + \lambda P_{n-1}(t) + \mu P_{n+1}(t) \tag{3}$$

But

$$\lim_{\Delta t \to 0} \left\{ \frac{P_n(t+\Delta t) - P_n(t)}{\Delta t} \right\} = 0 \text{ for stable condition}$$

Thus, the R.H.S. of equation (3) becomes

$$\mathrm{P}_{n-1}(t)\lambda - (\lambda+\mu)P_n(t) + P_{n+1}(t)\mu = 0 \tag{4}$$

To solve equation (4), it is assumed that there were 0 requests at time $t + \Delta t$. This can be obtained from the states as given under:

$$\begin{aligned} P_0(t+\Delta t) &= P_0(t)(1-\lambda\Delta t) \\ &= P_1(t)\mu\Delta t \\ &= P_0(t)(1-\lambda\Delta t) + P_1(t)(\mu\Delta t) \end{aligned}$$

$$\left(\frac{\left(P_n(t+\Delta t) - P_n(t)\right)}{\Delta t} \right) = P_n(t+\Delta t) = -P_0(t)\lambda + P_1(t)\mu \tag{5}$$

Thus, L.H.S. of equation (5) becomes

$$P_1(t) = \left(\frac{\lambda}{\mu}\right) P_0(t) \tag{6}$$

From equations (4) and (6), the following can be derived as:

$$\left.\begin{aligned} P_0(t) &= \left(\frac{\lambda}{\mu}\right)^0 P_0(t) \\ P_1(t) &= \left(\frac{\lambda}{\mu}\right)^1 P_1(t) \\ P_2(t) &= \left(\frac{\lambda}{\mu}\right)^2 P_2(t) \\ &\vdots \\ P_n(t) &= \left(\frac{\lambda}{\mu}\right)^n P_n(t) \end{aligned}\right\} \tag{7}$$

Summation of all the equations:

$$\sum\nolimits_{i=0}^{n} P_i(t) = \left\{\left(\frac{\lambda}{\mu}\right)^0 + \left(\frac{\lambda}{\mu}\right)^1 + \left(\frac{\lambda}{\mu}\right)^2 + \cdots + \left(\frac{\lambda}{\mu}\right)^n\right\} P_0(t) \tag{8}$$

Based on limiting condition, when $n \to \infty$ and $\frac{\lambda}{\mu} < 1$, L.H.S. becomes 1 and R.H.S. becomes $\left[\frac{1}{\left(1-\frac{\lambda}{\mu}\right)}\right] P_o(t)$.

Thus, equation (8) becomes

$$1 = \left[\frac{1}{\left(1-\frac{\lambda}{\mu}\right)}\right] P_0(t) \tag{9}$$

Substituting equation (9) in equation (8), we get

$$P_n(t) = \left(\frac{\lambda}{\mu}\right)^n \left(1-\frac{\lambda}{\mu}\right) \tag{10}$$

For variable n the average value can be written as:

$$\begin{aligned} Q(n) &= \sum_{n\to\infty}^{N} nP_n(t) \\ &= \sum\nolimits_{n\to\infty}^{N} \left(\frac{\lambda}{\mu}\right)^n \left(1-\frac{\lambda}{\mu}\right) = \left(1-\frac{\lambda}{\mu}\right) \sum\nolimits_{n\to\infty}^{N} \left(\frac{\lambda}{\mu}\right)^n \end{aligned} \tag{11}$$

Expanding equation (12), we get

$$= \left(1-\frac{\lambda}{\mu}\right)\left\{\frac{\lambda}{\mu}+2\left(\frac{\lambda}{\mu}\right)^2+3\left(\frac{\lambda}{\mu}\right)^3+\cdots\ldots\right\}$$

$$\equiv \left(1-\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)\left\{1+2\left(\frac{\lambda}{\mu}\right)^1+3\left(\frac{\lambda}{\mu}\right)^2+\cdots\ldots\right\}$$

Representing the equation in terms of differentiation, we get

$$\left(1-\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)\frac{d}{d\left[\frac{\lambda}{\mu}\right]}\left\{\frac{\lambda}{\mu}+\left(\frac{\lambda}{\mu}\right)^2+\left(\frac{\lambda}{\mu}\right)^3+\cdots\ldots\right\}$$

$$\equiv \left(1-\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)\frac{d}{d\left[\frac{\lambda}{\mu}\right]}\left\{\frac{\frac{\lambda}{\mu}}{1-\frac{\lambda}{\mu}}\right\}$$

$$\left(1-\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)\left\{\frac{\left(1-\frac{\lambda}{\mu}\right)+\frac{\lambda}{\mu}}{\left(1-\frac{\lambda}{\mu}\right)^2}\right\}$$

$$Q(n)=\frac{\left(\frac{\lambda}{\mu}\right)}{\left(1-\frac{\lambda}{\mu}\right)} \tag{12}$$

Equation (12) measures the average number of blocks at a given time.

3.1 Estimation of waiting time for blocks to be in blockchain

The average waiting time, $W(t)$, for the block is expected time required for the block(s) to be part of blockchain network, and is mathematically expressed as:

$$\begin{aligned} W(t) &= \frac{1}{\mu}\left(\frac{\text{Ø}}{1-\text{Ø}}\right), \text{ where } \text{Ø}=\frac{\lambda}{\mu} \\ &= \frac{1}{\mu}\left[\frac{\lambda}{\mu}\left(1-\frac{\lambda}{\mu}\right)\right] \end{aligned} \tag{13}$$

Equation (13) describes the average waiting time of one confirmation.

4 Experiment outcomes

The close connection of Markov model with time and its correlation with exponential distribution has caused the model to be applied for analysis of waiting time of blocks.

The exponential distribution is suitable for the problem, as inclusion of previous block in blockchain is independent of next block. Table 2 illustrates the outcomes of result based on equation (13) with four different confirmations.

Table 2 Outcomes of equation (13)

λ	μ	*Waiting time*			
		1 confirmation	*3 confirmations*	*6 confirmations*	*60 confirmations*
1	2	0.25	0.75	1.5	15
2	3	0.222222222	0.666666667	1.333333333	13.33333333
3	4	0.1875	0.5625	1.125	11.25
4	5	0.16	0.48	0.96	9.6
5	6	0.138888889	0.416666667	0.833333333	8.333333333
6	7	0.12244898	0.367346939	0.734693878	7.346938776
7	8	0.109375	0.328125	0.65625	6.5625
8	9	0.098765432	0.296296296	0.592592593	5.925925926
9	10	0.09	0.27	0.54	5.4
10	11	0.082644628	0.247933884	0.495867769	4.958677686

The result displays that for obtaining six confirmations, block requires 1.5 minutes (= 90 seconds), which is relatively high seeing the current transaction systems. Solution seems to be advantageous associating to current blockchain system.

5 Conclusions

The outcomes mentioned in Table 2 depict significant improvement of blocks inclusion. The current system was tested with lone ten nodes and on test environment, with the following settings:

1. ergodic condition ($\lambda < \mu$) was followed throughout the test
2. orphaned blocks were not deliberated for the study
3. only M/M/1 queue was considered between transactions and inclusion.

The study can be further expounded using other queue models and with more number of nodes for result precision and enactment.

References

Agrawal, J. (2018) *8 Benefits of Blockchain to Industries Beyond Cryptocurrency Entrepreneur*, 18 January [online] https://www.entrepreneur.com/article/306420 (accessed 16 May 2018).

Akcora, C.G., Gel, Y.R. and Kantarcioglu, M. (2017) *Blockchain: A Graph Primer*, ArXiv170808749 Cs, August.

Altcointoday.com (2017) *Bitcoin and Ethereum vs. Visa and PayPal – Transactions per Second*, Altcoin Today, 22 April 2017.

Baliga, A. (2017) *Understanding Blockchain Consensus Models* [online] https://semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf (accessed 10 April 2018).

Bitcoin (2017) *3 Things to Know about Bitcoin Confirmations*, Bitcoin Confirmations [online] https://www.buybitcoinworldwide.com/confirmations/ (accessed 24 May 2018).

de Leon, D.C., Stalick, A.Q., Jillepalli, A.A., Haney, M.A. and Sheldon, F.T. (2017) 'Blockchain: properties and misconceptions', *Asia Pac. J. Innov. Entrep.*, December, Vol. 11, No. 3, pp.286–300.

Efanov, D. and Roschin, P. (2018) 'The all-pervasiveness of the blockchain technology', in *Procedia Computer Science*, Vol. 123, pp.116–121, https://doi.org/10.1016/j.procs.2018.01.019.

Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C. and Vines, J. (2018) 'Making sense of blockchain applications: a typology for HCI', in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, pp.458:1–458:14.

Faour, N. (2018) *Transparent Voting Platform Based on Permissioned Blockchain*, ArXiv180210134 Cs, February.

Feld, S., Schönfeld, M. and Werner, M. (2016) 'Traversing bitcoin's P2P network: insights into the structure of a decentralised currency', *Int. J. Comput. Sci. Eng.*, Vol. 13, No. 2, pp.122–131, January.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaría, V. (2018) 'Blockchain and smart contracts for insurance: is the technology mature enough?', *Future Internet*, February, Vol. 10, No. 2, p.20.

Hull, R. (2017) 'Blockchain: distributed event-based processing in a data-centric world: extended abstract', in *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, New York, NY, USA, pp.2–4.

Iansiti, M. and Lakhani, K.R. (2017) 'The truth about blockchain', *Harvard Business Review*, January–February, Vol. 95, No. 1, pp.118–127 (accessed 2 June 2018).

Jang, H. and Lee, J. (2018) 'An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information', *IEEE Access*, Vol. 6, pp.5427–5437, https://doi.org/10.1109/ACCESS.2017.2779181.

Karame, G.O., Androulaki, E. and Capkun, S. (2012) *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*, IACR Cryptology ePrint Archive, p.248.

Lewenberg, Y., Sompolinsky, Y. and Zohar, A. (2015) 'Inclusive block chain protocols', in Böhme, R. and Okamoto, T. (Eds.): *Financial Cryptography and Data Security*, Vol. 8975, pp.528–547, Springer Berlin Heidelberg, Berlin, Heidelberg.

Lin, J., Shen, Z. and Miao, C. (2017) 'Using blockchain technology to build trust in sharing LoRaWAN IoT', in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, New York, NY, USA, pp.38–43.

Martindale, J. (2018) Before Crypto Nirvana, Blockchain Needs to Solve these Basic Problems, Digital Trends, 16 April 2018 [online] https://www.digitaltrends.com/computing/blockchain-problems-how-to-solve-issues-with-the-latest-vogue-tech/ (accessed 25 May 2018).

Miers, I., Garman, C., Green, M. and Rubin, A.D. (2013) 'Zerocoin: anonymous distributed e-cash from bitcoin', in *2013 IEEE Symposium on Security and Privacy*, pp.397–411.

Milano, A. (2018) *Walmart Wants Blockchain to Make Shipping 'Smarter'*, CoinDesk, 2 March 2018 [online] https://www.coindesk.com/walmart-using-blockchain-tech-make-shipping-smarter/ (accessed 16 May 2018).

Nash, K.S. (2018) 'Business interest in blockchain picks up while cryptocurrency causes conniptions', *WSJ* [online] https://blogs.wsj.com/cio/2018/02/06/business-interest-in-blockchain-picks-up-whilecryptocurrency-causes-conniptions/ (accessed 26 May 2018).

Neumayer, S., Varia, M. and Eyal, I. (2018) *An Analysis of Acceptance Policies for Blockchain Transactions*, No. 040 [online] http://eprint.iacr.org/2018/040 (accessed 27 May 2018).

O'Sullivan, K. (2018) *Blockchain in Air Travel | SITA*, SITA: Create Success Together [online] https://www.sita.aero/resources/blog/blockchain-in-air-travel/ (accessed 13 May 2018).

Pepijn, D. (2017) *5 Ways Blockchain Tech Can Benefit Businesses* [online] https://www.business.com/articles/5-business-benefits-of-blockchain/ (accessed 16 May 2018).

Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G. and Herrera Joancomartí, J. (2018) 'Double-spending prevention for bitcoin zero-conformation transactions', *International Journal of Information Security*, DOI: 10.1007/s10207-018-0422-4.

Sherman, L. (2017) *Five Issues Preventing Blockchain from Going Mainstream: The Insanely Popular Crypto Game Etheremon is One of Them*, Forbes [online] https://www.forbes.com/sites/gradsoflife/2018/05/03/workforce-wins-finding-the-right-candidate-in-less-time/#2e71ebff783e (accessed 2 June 2018).

Shi, N. (2016) 'A new proof-of-work mechanism for bitcoin', *Financ. Innov.*, December, Vol. 2, No. 1, p.31.

Srivastava, R. (2013) 'Evaluation of response time using gang scheduling algorithm for B2C electronic commerce architecture implemented in cloud computing environment by queuing models', *Int. J. Future Comput. Commun.*, Vol. 2, No. 2, pp.71–75.

Stifter, N., Judmayer, A., Schindler, P., Zamyatin, A. and Weippl, E. (2018) Agreement with Satoshi – On the Formalization of Nakamoto Consensus, Report No. 400, IACR [online] http://eprint.iacr.org/2018/400 (accessed 2 June 2018).

Wüst, K. and Gervais, A. (2017) *Do you need a Blockchain?*, Report No. 375, IACR [online] http://eprint.iacr.org/2017/375 (accessed 24 May 2018).

www.valtech.com (2018) *Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains* [online] http://www.maersk.com/en/press/press-release-archive/maersk-and-ibm-to-form-joint-venture (accessed 16 May 2018).