

Blockchain Technology and Cryptocurrency

Scaria Alex, T DhiliphanRajkumar

Abstract— As the online transactions are growing the security and new technological advancements are a recent concern. A decentralized architecture and distributed computing paradigm have given birth to cryptocurrencies that embed the blockchain technology. Bitcoin is one such currency which is revolutionizing the digital transaction field. The asymmetric cryptography is used to register and transfer the cryptocurrencies along with various algorithms like Proof-of-stake and Proof-of-work. The main advantage of the method is difficulty in counterfeiting, destroying and mining the currencies. In this paper, a detailed study on cryptocurrency and blockchain is carried out giving an oversight to the emerging technology. The recent trends have results showing the emergence of mobile cryptocurrency based digital transactions to be of higher rate due to the high popularity of Bitcoin and Ethereum. The use of Bitcoins and other cryptocurrencies have lured the transaction costs.

Keywords—Bitcoin, Cryptocurrency, Blockchain, Decentralized, Distributed.

I. INTRODUCTION

A digital money (or cryptographic money) is an advanced resource which help to overcome the defects of the trade utilizing cryptography to verify the money exchanges, controlling the extra units created and to verify the exchange benefits. The money in the form of the cryptocurrency are a kind of virtual monetary standards. The blockchain which is the decentralized control of the digital money which works as a disseminated record through an open database exchange.

The system to be a cryptocurrency should meet the following six conditions:

- The framework doesn't require a focal expert, dispersed accomplish accord on its state.
- The framework keeps an outline of cryptographic money units and their possession.
- The framework characterizes whether new digital money units can be made. On the off chance that new digital currency units can be made, the framework characterizes the conditions of their birthplace and how to decide the responsibility for new units.
- Cryptocurrency ownership to gadgets may be exclusively provided.

- The cryptographed units will be changed when the device lets in transactions. The cutting-edge ownership of the devices will announce the digital transaction.
- The gadget plays at maximum one if two or more exclusive commands arrive for converting the ownership of a cryptographic device concurrently.

The decentralized cryptocurrency is generated by way of the whole gadget on cryptocurrency collectively, in a rate associated with the gadget when its created and is publicly known. The supply of currency is manipulated by the government, centralized banking and monetary bodies like reserve bank by printing fiat money or providing digital banking ledgers. The blockchain based cryptocurrencies have blocked the businesses or government from producing new units exemplarily and for till now haven't backed any firm who plays a good role in the field. Satoshi Nakamoto, a group of individuals is the sole responsible for creating the underlying technicality of blockchain.

Approximately around a thousand cryptocurrencies exist as of October 2017. Majority of these digital currencies follow the spec and protocols of the primary centralized and fully executed currency called bitcoin. The miners are a group of mutually distrustful events who take care of the safety, integrity and balance of ledgers. In accordance with a particular timestamping scheme the participants in the miners validate and timestamp the whole transactions made. The security of the blockchain based cryptocurrency is the sole responsibility of miners and they in turn achieve an incentive.

The design of most of the cryptocurrencies are based on to decrease manufacturing offorex, putting a full stop on the full amount of currencies to be able to be in circulation mimicking previous metals (Andy, 2011). It will be very difficult to seizure cryptocurrency through regulation enforcement which when compared with everyday currencies held in financial institutions (Andy, 2011). The cryptographic technology will leverage this derived issue. The Silk Road case is a number one example of the assignment of regulations, in which Ulbricht's bitcoin stash "was held on by one and encrypted"[8]. The true anonymity can be achieved by blockchain based cryptocurrencies like bitcoin together with zerocoin.

II. RELATED WORKS

"b-cash", a nameless, dispensed electronic coins system was proposed by Wei Dai in 1998 [10]. "bit gold" was latter developed by Nick Szabo.[11] Bit Gold, a follower of bitcoin and other cryptocurrencies, became a digital foreign money gadget which need the customers to finish a proof of

Revised Manuscript Received on December 05, 2019.

Dr. T DhiliphanRajkumar, Assistant Professor Department of Computer Science and Engineering, Kalasalingam University

Mr. Scaria Alex Research Scholar Department of Computer Science and Engineering, Kalasalingam University

work characteristics with solutions being cryptographically prepared and published. Hal Finney who followed the work and achievements of Dai and Szabo created a fully reusable proof of work based cryptocurrency. Satoshi Nakamoto, a pseudonymous developer created the first decentralized blockchain based cryptocurrency in 2009. As its proof-of-workings scheme a cryptographic hash function named SHA-256 is used [12]. Namecoin was formulated in the year April 2011 created as a trial attempt on forming a decentralized Domain Name Servers (DNS) which ultimately will help in making censorship in the internet difficult. In October 2011 Litecoin was launch which utilized script as the hash features instead of SHA-256. This cryptocurrency was a huge success. Another great cryptocurrency, Peercoin was the primary to apply hybrid evidence-of-workings / evidence-of-stake [13]. The first cryptocurrency which is no longer available is the Distributed ledger technology (IOTA).

III. PROPERTIES OF CRYPTOCURRENCY

Bitcoin is surely a decentralized cryptographic network of friends who keep watch on the consensus of the account and balances. It is like a foreign money that is similar to the numbers seen on the financial institution accounts. It is actually a entries on a database which will be changed by means of unknown people which are bound through a set of rules or protocols. The cryptocurrencies are a decentralized consensus-database entries.

A. Transactional properties

Irreversible: A transaction can't be reversed after the confirmation by no one. And nobody approach no person. The data once entered cannot be manipulated by any associated person once its committed, not even by the developer Satoshi or the miners. If the transaction is done then its done and if the data been stolen by hacker it will be of no much accessibility by them.

Pseudonymous: The transactions or the account is not related to any of the real international identities. The bitcoins are received on the processing addresses that are randomly generated with among 30 characters chained together. The transaction float can be investigated but it isn't always possible to connect the identification of customers in the real world with the generated addresses.

Fast and international: The propagation speed of the transactions are too high that the change is visible within minutes of its access. It is totally indifferent within the bodily location as the manifest is in a global community of

each proprietor must agree to. To understand the working of cryptocurrency a few principles have to be understood.

Specifically:

A. Public Ledgers:

In a public ledger all transactions from the beginning of a cryptographic currence creation are saved. The coin owners identities are encrypted and the machine makes use of the cryptographic strategies for file preserving to ensure legitimacy. To correct spendable stability the ledger calculates and ensures the corresponding digital wallets. For each transactions are checked with to make that every

networked computers. It have no difference if the bitcoin is sent to how long the distance be.

Secure: A public key cryptographic gadget locks the cryptocurrency finances. Only using the personalized private key can unlock the cryptocurrency. The use of SHA-256 will help in safe locking of the cryptocurrency. A bitcoin uses Fort Knox which is more secure than any algorithms.

Permissionless: Cryptocurrency is a software that everyone should use and download for free. After the installation, the bitcoins could be mined and used for transactions. There is no blockage or rules for governing the installation of cryptocurrency. Its open source and anyone can use.

B. Monetary properties

Controlled deliver: The token supply is restricted by most of the cryptocurrencies. But in the case of bitcoin the supply decreases as time evolves and could even reach to an end in developing coins by the end of the year 2140. Using a timetable written in a code the supply of tokens is controlled. This approach results in large decline of the supply of the cryptocurrency in the mere future resulting in controlled circulation of monopoly.

No debt however bearer: The Flat-cash in the bank or the reserve government organisations are generated from the aid of the debt. Its generated as part of the IOU. The cryptocurrencies doesn't represent the amount of money owed but they constitute themselves. They are cash which is hard to attain same as extracting gold from the mines.

A permissionless, pseudonymous and irreversible manner of digital currency is a big challenge to the current technology flat-money bank monetary transactions. All the transactions are recorded and cannot be reverted and fully controlled by the person who generated the coin and the government or other monetary organizations have no control over the transactions.

IV. WORKING OF CRYPTOCURRENCY

After Cryptocurrencies like Bitcoin are in essence a sequence of digital 'tokens' that may be exchanged much like ordinary money besides all of the transactions take place over the net.

Unlike normal money, Bitcoin isn't regulated with the aid of any person or saved in banks. Instead it follows a shared set of guidelines that

transaction uses the most simplest coins that are currently owned by the spender. The bitcoin uses this public ledger which is called as a transaction block chain.

B. Transactions:

Transaction is called as a switch of price range between two or more virtual wallets. The committed transaction is then transferred to the public ledger and waits for a confirmation response. When the transaction is committed, the wallet uses

an encrypted data called as a cryptographic signature to offer a proof that has a valid mathematical solution which informs and identify the transaction is from an authorized personal of the wallet. The confirmation system then takes around ten minutes for bitcoins to confirm the transaction and enlists the miners about the event.

C. Mining

In easy phrases, the technique behind confirming the transactions and also including the public ledger onto the event is called mining. An increasingly more computational complex problem like a mathematical puzzle has to be solved by the miner to add a transaction to the ledger. The transaction could be verified by anyone as the whole process is open source. A block on the transaction is recorded by the first miner who could solve the puzzle and is pointed to the ledger. The transaction, the general public blockchain ledger paintings and blocks together guarantees that nobody could ever change the created block at ease without solving the mathematical puzzle. Once the ledger have a block to process, all related transactions are correlated and an appreciable transaction rate is accounted to the wallet of miners. This is called as the proof of work gadget as which is received by the miners as a token of appreciation. Thus the coins are mined.

D. Blockchain

Blockchain helps in validating every cryptocurrencies in the market. The blocks which are the core of a blockchain is a list of statistics that are securely linked using a cryptographic algorithm. Each block in the blockchain carries a hash pointer which points to the previous block. It also contains a timestamp which stores the creation time of the block and facts about the transaction. The modification of the facts are totally restricted by the properties of blockchain. The dispensed ledger which is open source code is responsible for the file transaction among various events. These events are verifiable and are permanent in manner. A blockchain is managed through a peer-to-peer community together with adhering to a set of protocols that could be used to validate new blocks. All these has to be done to use it as a disbursed ledger. Once all the specifically to them. They record the transaction, stamp the details and mark them as reliable and disclose within the network reach ability. After each transaction is passed and processed by a miner, it has to be recorded into the database. Thus each record block becomes a part of the blockchain.

VI. SECURITY

There are foremost approaches the blockchain ledger could somehow corrupt the blocks and steal the crypto coins by behaving fraudulently modifying or adding contents to the block. The crypto cash machine does its best on protecting the blockchain in opposition to each the usage of a mixture of digital signature in combination with cryptographic hash function.

A. The Addition Attack and Digital Signatures

The bitcoin providers and buyers are diagnosed within the blockchain by means of a public cryptographic key which most of the crypto coins could use to transfer from

transaction related information is recorded, it could never be able to be modified, not even a single block, without altering all the subsequent blocks related to the modifying block. This modification could result in collusion of the majority of the network. Blockchain have a high rate of Byzantine fault tolerance which eases it through the design. Blockchain follows the distributed computing technology. Blockchain have the capability of the decentralized technology. Without the need of a dependent authority or a server it can solve the double spending problem with ease.

V. CRYPTOCURRENCY MINING

Production of cryptocurrencies isn't always some thing like that of regular money. There's no central authority that troubles new notes; alternatively, bitcoins (or litecoins, or any of the other so-called 'alt-coins') are generated through a system referred to as 'mining'. In this chapter, the working of cryptocurrency is discussed.

A. How miners create coins

The meaning of transaction is that a file has been transferred in a manner, abc gave n bitcoins to xyz and all these cryptocurrencies are signed with abc's private key. The bitcoin uses the blockchain concept with the asymmetric cryptographic solution. After the coins been signed, a transaction can be broadcasted along the network which is send from a single peer to each individual peers available. This is the basic concept which is followed by the peer-to-peer methodology. The transaction is understood and recorded by the whole network with ease within that second. The critical concept related to cryptography and coin crypted is the confirmation.

The blockchains are referred as a lengthy transaction which is never unconfirmed and the pending confirmations will be casted at the earliest. When a transaction happens, its recorded in the block and it can never be reversed and becomes a part of an immutable document.

Transaction could be verified only by the miners which is a job that has been allotted

one public key to another specified public key. Crypto coin addresses which are a set of hashes of the defined public keys are used for this purpose. In reality, its possible for an attacker abc to steal cashes from n number of people by just including a transaction details to the blockchain ledger. The details could be like xyz will be paying abc a hundred crypto coins, ert will be paying abc a hundred crypto coins and so on, using of path these human's crypto coins addresses as opposed to the defined names. The protocol that governs the cryptographic coins prevent such activities though digitally signing every single switch in the network with the providers private key. Thus only the signed transfers could be introduced to the cryptographic coin ledgers. Thus only personals with authorized private key and public key combination could send and modify the contents in a block. A modification in public key is globally recognized and hence it will be not so easy to hack into a block and modify the data.

B. The Modification Attack and Mining

The different essential manner to thief crypto coins is probably to modify blockchain entries. Eve ought to purchase some thing from abc, like a settee, via including a privately signed key to the blockchain ledger which is equivalent to xyz can pay abc 100 crypto coins. Later, after the couch being received, xyz could regulate that blockchain ledger entry to verify further: xyz will pay abc 10 crypto cash, or even modify the entry. xyz can definitely signal her entry once more after enhancing it.

To save you against modification assaults, the crypto cash gadget first calls for entries be delivered to the blockchain not separately, but in groups or blocks. Most important aspect is that, every block should be followed by a cryptographic hash of 3 matters: the hash value of the previous block, the block, and various called a nonce. A hash function of best the first block will be, like several cryptographic hash, constantly have a hard and fast variety of bits like in SHA-256.

The cryptographic hashes are generated randomly inside the experience that most of their output can not be predicted from the defined inputs. The simplest solutions are regarded as the manner to locate the nonce which tries the integers followed by other integers. As the range of zeros increases it becomes more and more difficult to discover an default nonce. The crypto coins device periodically adjusts the range of zeroes so that the time taken to discover a nonce will always change dynamically. In this manner, as such the pc hardware are getting upgraded each year in a fast growing ratio the crypto cash protocol is also modifying its number of zero bits to accomplish the toughness in mining. Thus

D. Type of Attacks

Race attack: While having a transaction, but doesn't have a confirmation, stores and services depending on the transaction could be exposed to an attack called race attack. For instance if the transactions are generated for an equal price range which is to be send to one-of-a-kind shops/offerrings. Shops will be taking several premeasures to supress such forms of attacks. It is hence right to don't forget whether or not it must be given transactions with nonce affirmation.

Finney attack: It is another variants in the list of attacks. The affected personals are shops or services who has been given with transactions that are not confirmed. A finney assault send the money to the defrauder by calling a block called minerto premine. The risk of these type of attacks cannot be reduced to zero even how much preventive measures we have chosen. But it actually requires the participation of a lot of miners and a matching combination of contriuting factors. Here the miner is the reason who dangers the capability of a secure block.

Vector76 attack: This attack is also called as an attack with confirmation. It is an aggregate of the two previously mentioned attacks which helps the offender in spending funds multiple times with confirmation.

making an attacker more difficult in recalculating all the hashes of a single block after the one that has been modified. Thus for example, if xyz desires to exchange a hundred crypto coins to one bitcoin, she will be able to now not simplest just have to recalculate the hash value of each block used in transaction and also have to process all blocks that are assigned along with the block. It will take a lot of time to process and as the time flies the people will be adding more and more block to the chain. Thus its going to accomplish a whole lot quicker that xyz on my own can mine. Xyz might must recalculate all of the blocks before the community ought to reload a brand new one, or as a minimum follow up and catch up with he network miners. Thus the system have the capability to protect itself from the fraudulent blockchain adjustments via making them more difficult to nonce by adding more complex hash values. As the number of miners increases the possibility of such an attack reduces as much more blocks ae generated in a second.

C. Double-Spending

Crypto cash device is primarily based on a modern answer of a hassle not unusual to all digital foreign money and charge schemes: which is for such called as double-spending. With virtual money, that's just a pc record, this isn't always the situation, and the provider may want to in precept buy the identical cash again, copying the report time and again. With crypto coins, when xyz offers to pay abc a few crypto coins, abc could usually first verify the blockchain ledger to confirm that xyz truely is the owner that many crypto coins. However crypto cash can block towards that. If xyz offers to pay abc a few crypto coins in exchange for goods, abc can manipulate that she would now not supply the goods till xyz charge to abc appears within the blockchain, which mostly includes ready within ten mins.

Brute force attack: This assault is feasible despite the fact that the store or carrier is anticipating numerous confirmations over the transaction. Here the attacker will be in a possession of notably excessive-high performing hardware.

The perpetrator does two things here, one is sending a transaction to the shop to be attacked by delivering a product or provider and secondly will be seeking out a blockchain connection. Both the activity happens within he same stipulated time. The blockchain fork will be broken and attains all the cashes, but if the legitimate owner has failed in acheiving it, the attack will totally a failure.

The achievement of this assault is based on how fast the hash frequency of the assaulter is and the wide variety of success rate for the store/carrier. For instance, lets imagine the attacker acquire 10% of the energy calculated of the crypto cash networkig and the store is anticipating six success rate of a successful transaction, the chance of success rate of the assault might be only 0.1%.

VII. LIST OF CRYPTOCURRENCIES

The quantity of cryptocurrencies to be had over the internet as of 10 April 2018 is over 1565 and developing. A new



cryptocurrency can be developed with ease at any time. By marketplace capitalization, Bitcoin is currently (April 10,2018) the biggest blockchain network,observed by using Ethereum, Ripple, Bitcoin Cash, Litecoin, and EOS.

Bitcoin: It is the best and most widely used famous cryptocurrency available in the market. It is considered as a digital digged gold popular within the organizations affiliated to cryptocurrency. It is currently used as a defacto for the foreign money of the cyber warfare like darknet or ransomware. The rate of bitcoin is increasing daily with a day to day transaction crossing more than 200,000.

Ethereum: Vitalik Buterin developed this crypto currency and is standing at the second position among the best digital coins. The bockchain technique of this digital coin doesn't effectively validate the accounts and balances of the current state. This released a complication over the contracts and various other applications.

Ripple: It is an ill famous or not much popular crypto currency. The ripple is a community that developed a digital currency XRP. It is the community that constulated IOUs rather than using crypto currencies. XRP is the default currency of the ripple community.

XRP tokens are generated by Ripple labs, which is a community consisting of ripple network and is transferred in will for utilization. This currency is also known as a varities of crypto currencies with their personal upgrades, but any of them did ever gain the identical reputation as Monero.

VIII. CONCLUSION

Same as paypal or bank credits the cryptocurrencies could be considered as a digital currency used for online transactions. A digital ledger is the responsible item over recording the digital transactions and balances which is in term called as blockchain. Wallets are the softwares used to access the cryptocurrencies. The transactions ae created within the wallets which are broadcasted to the whole network which inturn is added onto the blockchain. Through the online exchanges of cryptocurrency or with the help of a broker the crypto currencies could be bought. There are many other cryptocurrencies beyond Bitcoin. The digital currency like bitcoin which implement cryptography over blockchain are decentralized and hence is entirely different from flat currencies provided by banks and other government organizations. An algorithm and the miners are the personals who have the sole control over the digital currency rather than a centralized power. The working of the crypto currency related to the transactions are defined by the algorithm. It also defines when the coins to be generated. With the organized use of wallets the users does transactions in a peer-to-peer manner. The public digital ledger records the transactions. Miners are those who breaks the cryptographic codes to confirm the transaction. The new coins are generated when a mining is done.The ease of using digital currency like bitcoin will revolutionize on how the digital transactions are gonna happen in the mere future.

premined cryptocurrency with a network and have less concern over shop fees. Its never been a part of real world transaction.

Litecoin: If bitcoin is the digital gold then the digitl silver is awarded to litecoin. It is very much faster than bitcoin and have a huge amount of tokens burried under with a brand new rules over the mining. Litecoin is a real revolution which have perfectly conquered the title of second best to bitcoins. The dogecoin and feathercoin are developed from the code base of litecoin and made much faster and lighter digital currencies.

Litecoin is considered to be a back up plan if the bitcoin fails. For now the bitcoin is ruling the world as the litecoin have no much user base. But even then its an actively developed community.

Monero: If the crypto currency have a maximum collection of rules to govern its circulation and development, then its only associated to Monero. Bitcoin had a disadvantage over the issue of the privatisation which is rectified oer this particular algorithm. With the evolution of a new idea referred to as ring-signatures, the cryptonite set of rules changed into premined and as a consequence rejected with the aid of the community. Monero is similar to bytecoin in the context that it is also a non-premined and raised quite a few consciousness. There are several different

REFERENCES

- [2] M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA: O'Reilly Media, 2015.
- [3] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
- [5] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
- [6] C. L. P. Chen and C.-Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on big data," *Inf. Sci.*, vol. 275, pp. 314–347, Aug. 2014.
- [7] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- [8] [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [9] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, 2016, pp. 2663–2668.
- [10] F.-Y. Wang, "Blockchain intelligence: Cornerstone of the future smart economy and smart societies," in *Proc. 2nd World Intell. Congr.*, Tianjin, China, 2018.
- [11] *Blockchain Monitoring Website*. Accessed: Jan. 8, 2016. [Online]. Available: <https://blockchain.info/>
- [12] *Cryptocurrency Monitoring Website*. Accessed: Nov. 24, 2015. [Online]. Available: <http://coinmarketcap.com/>

AUTHORS PROFILE

Dr. T DhilliphanRajkumar



Assistant Professor
Department of Computer Science and
Engineering, Kalasalingam University
Mr. Scaria Alex
Research Scholar
Department of Computer Science and
Engineering, Kalasalingam University

- [10] World Economic Forum Survey. Accessed: Feb. 21, 2016. [Online]. Available: <http://www.coinfox.info/news/3184-world-economic-forum-survey-10-of-global-gdp-may-be-stored-with-blockchain-technology-by-2027>
- [11] CoinDesk Report. Accessed: Feb. 21, 2016. [Online]. Available: <http://www.bitcoin86.com/news/3527.html>
- [12] N. Modiri, "The ISO reference model entities," IEEE Netw. Mag., vol.5, no. 4, pp. 24–33, Jul. 1991.
- [13] X. Wang, L. X. Li, Y. Yuan, P. J. Ye, and F.-Y. Wang, "ACP-based social computing and parallel intelligence: Societies 5.0 and beyond," CAAI Trans. Intell. Technol., vol. 1, no. 4, pp. 377–393, 2016.
- [14] X. Wang, X. H. Zheng, X. Z. Zhang, K. Zeng, and F.-Y. Wang, "Analysis of cyber interactive behaviors using artificial community and computational experiments," IEEE Trans. Syst., Man, Cybern., Syst., vol. 47, no. 6, pp. 995–1006, Jun. 2017.
- [15] F.-Y. Wang, Y. Yuan, X. Wang, and R. Qin, "Societies 5.0: A new paradigm for computational social systems research," IEEE Trans.Comput. Social Syst., vol. 5, no. 1, pp. 2–8, Mar. 2018.
- [16] T. V. Lakshman and A. K. Agrawala, "Efficient decentralized consensus protocols," IEEE Trans. Softw. Eng., vol. SE-12, no. 5, pp. 600–607, May 1986.
- [17] C. L. P. Chen, G.-X. Wen, Y.-J. Liu, and F.-Y. Wang, "Adaptive consensus control for a class of nonlinear multiagent time-delay systems using neural networks," IEEE Trans. Neural Netw. Learn. Syst., vol. 25, no.6, pp. 1217–1226, Jun. 2014.
- [18] J. Fan, L. T. Yi, and J. W. Shu, "Research on the technologies of Byzantine system," J. Softw., vol. 24, no. 6, pp. 1346–1360, 2013.
- [19] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Netw. Appl., vol. 9, no. 2, pp. 397–413, 2016.
- [20] Y. Yuan, F.-Y. Wang, and D. Zeng, "Competitive analysis of bidding behavior on sponsored search advertising markets," IEEE Trans. Comput. Social Syst., vol. 4, no. 3, pp. 179–190, Sep. 2017.
- [21] Y. Yuan, D. Zeng, H. M. Zhao, and L. J. Li, "Analyzing positioning strategies in sponsored search auctions under CTR-based quality scoring," IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 4, pp. 688–701, Apr. 2015.
- [22] J. J. Li, X. C. Ni, and Y. Yuan, "The reserve price of ad impression in multi-channel real-time bidding markets," IEEE Trans. Comput. Social Syst., vol. 5, no. 2, pp. 583–592, Jun. 2018.
- [23] F.-Y. Wang, Y. Yuan, C. M. Rong, and J. J. Zhang, "Parallel blockchain: An architecture for CPSS-based smart societies," IEEE Trans. Comput. Social Syst., vol. 5, no. 2, pp. 303–310, Jun. 2018.
- [24] Y. Yuan, T. Zhou, A. Y. Zhou, Y. C. Duan, and F.-Y. Wang, "Blockchain technology:From data intelligence to knowledge automation," Acta Automatica Sinica, vol. 43, no. 9, pp. 1485–1490, 2017.
- [25] S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: A survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2014.
- [26] K. Dorling, J. Heinrichs, G. G. Messier, and S. Magierowski, "Vehicle routing problems for drone delivery," IEEE Trans. Syst., Man, Cybern., Syst., vol. 47, no. 1, pp. 70–85, Jan. 2017.
- [27] H. Li, D. H. Pan, and C. L. P. Chen, "Intelligent prognostics for battery health monitoring using the mean entropy and relevance vector machine," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 7, pp. 851–862, Jul. 2014.
- [28] D. Wen, Y. Yuan, and X.-R. Li, "Artificial societies, computational experiments, and parallel systems: An investigation on a computational theory for complex socioeconomic systems," IEEE Trans. Services Comput.,vol. 6, no. 2, pp. 177–185, Apr./Jun. 2013.
- [29] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]," IEEE Technol. Soc. Mag.,vol. 34, no. 4, pp. 41–52, Dec. 2015.
- [30] La'zooz Website. Accessed: Feb. 2, 2018. [Online]. Available: <http://www.lazooz.org/>
- [31] Arcade City Website. Accessed: Feb. 2, 2018. [Online]. Available: <http://arcade.city/>