Application of Cryptocurrencies using Blockchain for E-Commerce Online Payment

Kayode Adewole[1], Neetesh Saxena[2], Saumya Bhadauria[3]

[1]Department of Computing and Informatics, Bournemouth University, UK

[2]School of Computer Science and Informatics, Cardiff University, UK

[3]Department of Computer Science, ABV-Indian Institute of Information Technology and Management, Gwalior, India

s4923248@bournemouth.ac.uk, nsaxena@ieee.org, saumya@iiitm.ac.in

Abstract

Due to the distinctive properties of the Blockchain, which is the decentralized and distributed ledger that used to record transactions done, the cryptocurrencies are being used as an online payment source in transactions. The cryptocurrencies attributable to their notable characteristics, such as decentralized consensus, anonymity, distributed and shared ledger, immutability, and autonomy, and are best managed with the Blockchain. However, similar to other payment sources, the Blockchain and cryptocurrencies are also prone to security attacks. The Blockchain technology itself faces abuses, such as links to child abuse contents, money laundering, tax evasion, financing illegal activities like sex and drugs, and terrorism.

In this research work, the practical reach of cryptocurrencies to people and its use as an investment option is studied by getting responses from people through a questionnaire. To understand the real-time security threats that people have of cryptocurrencies and the prospects of cryptocurrency as a potential investment, a questionnaire on cryptocurrencies and its applications, potential risks seen by people, and its likelihood as an investment option, is administered to a sample of 100 educated professionals. Analysis of responses shows that people are skeptical to adopt cryptocurrencies as online payment medium due to the security risks posed by it. The major security issues reported with cryptocurrencies are attacks on cryptocurrency wallet, time jacking, 51% attack, double spending, selfish mining, and fork issues. These issues are addressed by applying appropriate resolution techniques. Lack of common international governance and regulation has been found to be the primary cause of abuses of Blockchain technology. This mandates that the world community come together and lay regulations and policies for preventing abuses on Blockchain technology.

Keywords: Cryptocurrencies, Blockchain, online payment, security.

1. Introduction

E-commerce is conducting business and purchases online over the internet. E-commerce is done worldwide and new technologies make the transactions much more easy, secure, and sophisticated. There are many online payment methods in e-commerce, such as credit/debit card payment, direct debit payment, electronic funds transfer, electronic wallet payment, smart cards, and crypto-currency payment ("4.1 Electronic Payment Systems (EPS)" n.d.). Blockchains and cryptocurrencies are growing areas and hence they are being implemented in many applications.

Cryptocurrency is digital money or virtual money that is encrypted using cryptography for security. It is decentralized and is transferred between peers using a public ledger called Blockchain. Bitcoin is the first cryptocurrency. Blockchain is the main ledger that record and saves all activities on a cryptocurrency along with information about the owners. A cryptocurrency transaction is finalized only when it is added to the Blockchain. The payment transactions done with cryptocurrencies through Blockchains are secure as they are decentralized, do not need a third-party for transactions, have no risk of exchange, and are faster (Martucci 2018).

Many banks and financial institutions are exploring in areas like payments, asset registries, regulatory reporting, KYC, digital currency exchange, experimentation with digital security, gifts, and many others. Some banks and financial institutions experimenting with Blockchains are ANZ bank, Citibank, BNP Paribas Barclays Bank, EBA, Deutsche Bank, NASDAQ, and DBS bank ("Know more about Blockchain: Overview, Technology, Application Areas and Use Cases" 2018).

A. Security Issues:

Phishing and pharming are the general security issues with e-commerce payments. Security issues related to cryptocurrencies and Blockchains are time jacking attacks, ">50%" attacks, attacks on wallet software, double-spending, and selfish mining. These security attacks require fixations in cryptocurrency and Blockchain protocols and architecture, besides external security measures. It also has legal, governance, and data management safety implications. This research paper addresses these security issues and available existing solutions to overcome them (Vyas & Lunagaria 2014).

B. Research Problem:

The online payment process is being widely used due to the increased use of e-commerce transactions. New technologies like Blockchains are finding their way as a payment medium in online transactions. However, they are under evolution in many applications since the risks and security concerns in implementation are not yet known. This paper explores employing Blockchains as an online payment source, potential security problems, and the available solutions to overcome them. This study helps to locate where problems can arise in Blockchain payments and hence look for problematic areas in the future. This study will also benefit from understanding the financial process in online transactions.

The aim of this research is to do study the process of using Blockchains technology as an online payment medium and to find out the security issues that can arise in such an implementation process. The research objectives are:

- What are the security issues related to online payment process using Blockchains?
- Can the attack be classified?
- Find out the existing solutions for the identified security concerns

This chapter provides intuitive and comprehensive insights to the basics of cryptocurrency and blockchain technology. It covers all background aspects and the issues related to online payment process (with or without blockchain). Further, in context of online transactions the security and privacy attributes of blockchain are characterized. At later stage the attacks targeting the blockchain are discussed and their effects with possible defense mechanisms are identified.

2. Literature Work

This section discusses background study, possible security issues with the Blockchain and the existing solutions.

A. Background Study:

(i) Online Payment Process in E-Commerce

Transactions between buyers and sellers in e-commerce comprise of request for information, quotation of prices, placement of orders, payment processing, and notifications. All these operations need a high level of confidentiality, authenticity, security, and protection of privacy (Niranjanamurthy & Chahar 2013).

Online payments are not directly processed by the shopping sites, but generally, employ payment gateways. The payment gateways or transaction enablers establish business relationship with financial institutions to accept online payment for their merchant clients. PayPal, Google Checkout, and Authorize.Net are some of the major payment gateways used worldwide (Acosta 2008). Information transaction during payment processing between a customer and the merchant website should be in a secured manner.

Cryptocurrency is a digital or virtual currency created and stored electronically in Blockchains. Encryption techniques (cryptography) are used to create funds, regulate and verify the transfer of funds. It is not regulated or controlled by any bank or government and hence is decentralized. Popular cryptocurrencies are Bitcoin, Ethereum, Litecoin, Dash, and Peercoin. Cryptocurrencies have low transaction fees, offer identity protection, and are risk-free for sellers. However, they are volatile due to the fluctuating exchange rates and their newness into the market (“What is cryptocurrency — and how can I use it?” 2018). Cryptocurrency transactions are recorded in a digital public ledger called Blockchain or distributed ledger. Each record or a series of records on the Blockchain is called a block. Every user transaction in the network creates a block and is verified by all users of the network, which is then added to the Blockchain. A block cannot be changed once verified and added. Those

users working to record the transactions are called miners and they are paid in tokens for services rendered.

(ii) Blockchain as an Online Payment Method

a. Cryptocurrencies and Blockchain Technology

Cryptocurrencies are digital money that have found their way in many applications, including banking and e-commerce. Blockchain is the building blocks of the master ledger that records cryptocurrency transactions. This section discusses the concepts of Blockchain, its architecture, the key elements, its working principle, and the difference between Blockchains and traditional databases. Cryptocurrency is digital money or virtual money that is encrypted using cryptography for security. It is decentralized and is transferred between peers using a public ledger called Blockchain. Cryptocurrencies can be exchanged for fiat currencies in special online markets. They have a variable exchange rate with the world's major currencies like USD, British Pound, and European Euro. They have only a very finite supply (Martucci 2018).

The Blockchain of a cryptocurrency is a master ledger that records and stores all transactions and activities over that currency along with owner information. Identical copies of Blockchain are stored in every node of cryptocurrency's software network run by a group of individuals called miners. The miners pick up transaction records, verify their legitimacy and generate new blocks by executing cryptographic functions. The blocks are added to the previous blocks in the Blockchain and are irreversible. Each cryptocurrency holder has a private key to authenticate their identity and to exchange their units (Jaag & Bach 2016). A Blockchain is a distributed ledger formed by all completed transactions of cryptocurrencies in a network. It serves as a single source of truth of a network. A Blockchain is composed of a chain of data packages or blocks. A block comprises of multiple transactions. The first block is called the genesis block. Besides transactions, each bock consists of (Nofer et al. 2017):

- A timestamp
- The hash value of the previous block or the parent – Unique value and changes when blocks in a chain are changed
- A nonce, which is a random number to verify the hash

A Blockchain system has a number of nodes, each of which has a local copy of the ledger. The nodes communicate with one another to gain agreement with one another to add a Blockchain. The process of gaining this agreement is called consensus. When a chain is added, it is recorded in the ledger in all the nodes, gaining it the name of the distributed ledger. Once a record of a transaction is added in the Blockchain, it cannot be changed or removed. This property is called immutability.

The right to perform transactions in a Blockchain works on two models namely permissioned and permission-less models. Users must be enrolled in a Blockchain to perform transactions in a permissioned Blockchain. Any person can perform transactions in permission-less Blockchain, but

they can operate only on their own data ("Cloud Customer Architecture for Blockchain" 2017). The distributed ledger system helps the Blockchain to carry out its tasks even is a node is broken down. This increases trust in the system. Intermediaries are eliminated in Blockchain architecture and hence data security is fostered.

b. How Blockchain Works

The Blockchain is a shared ledger that stores transaction information in a distributed network of non-trusted peers. The transactions are performed by people in a Blockchain through their computers, called nodes. Each block in a Blockchain references the previous one and contains data, its own hash, and a hash of the previous block. Hash is a value generated from a string of text using a mathematical function and is unique. Though hash algorithm ensures the security of a block and Blockchain, a process called proof-of-work is also used to mitigate corruption and to enhance security. Proof-of-work (PoW) is a process of producing data that is hard to produce but easy for others to verify. The miners must complete a PoW or mathematical problem, for a block to be accepted by network participants. On average, performing PoW calculations and adding a new chain to the block takes about 10 minutes (Tania 2018).

Blockchain wallets are digital wallets where users can store their cryptocurrencies. Using the unique wallet ID assigned to their wallets. The wallet is composed of an address, called a public key, and a private key called the secret. A wallet generates paired public and private keys that ensure the safety of transactions.

Anyone can send a transaction using the public key to the address of the receiver. The owner of the wallet alone, who has the private key, only can access that transaction. Three principle technologies combine to create a Blockchain namely (1) private key cryptography, (2) a distributed network with a shared ledger, and (3) an incentive for servicing the network's transactions and record keeping. Identity in Blockchain is created by a combination of public and private cryptographic keys. The combination of these keys provides a strong digital signature leading to strong ownership. The miners perform transactions and create blocks which are sent to every node. The block is validated using PoW by the nodes and gets added to the Blockchain and ledger is updated. The nodes or miners get rewarded for these activities in the form of cryptocurrencies which are added to their digital wallet (Bauerle 2018). Payment gateways are also integrated into the transaction process. They scan the Blockchain to confirm the transaction.

c. Elements of Blockchain

The building blocks of Blockchain and the underlying technology behind Blockchain transactions shows that this is not a single technique, but is a combination of cryptography, mathematics, algorithm and economic model, a combination of peer-to-peer networks, and application of distributed consensus algorithm forming an integrated multi-field infrastructure construction. Blockchain technology is essentially composed of sex elements given under (Lin & Liao 2017):

- Decentralized – Blockchain does not rely on a centralized node but the data can be recorded, stored, and updated in a distributed manner
- Transparent – The records and blocks are transparent making Blockchain trustworthy
- Open Source – Most Blockchains are open to everyone. People can check records publicly and use Blockchain technologies to create any application
- Autonomy – Nodes are updated by consensus without any user intervention. The trust of safe data transfer and update is placed on the entire system and not just on a single person.
- Immutable – All records are reserved forever and cannot be changed unless somebody takes control of more than 51 % percent nodes simultaneously
- Anonymity – Data transfer and transactions can remain anonymous since only Blockchain addresses are needed for access and transfers.

d. Characteristics of Blockchain

Blockchain implementations aim for scalability and concurrency and want to ensure no single point of failure. They include pluggable components like databases and other consensus mechanisms. Their successful implementations come from multi-level confidentiality, privacy through multi-channel communication, multiple sub-ledgers, and multiple stakeholders. Blockchains have several characteristics that affect their architecture and implementation ("Cloud Customer Architecture for Blockchain" 2017):

- Cryptography – The trust and validity of Blockchain transactions are due to the cryptographic proofs and mathematical computations between various trading partners
- Immutability – Blockchain transactions cannot be deleted or altered
- Provence – The origin of every transaction in a Blockchain can be traced
- Decentralized computing infrastructure – Nodes are capable of making independent processing and computational decisions irrespective of the decisions of their peer nodes
- Distributed platform – This platform handles transactions like exchanging value, assets, or other entities
- Decentralized database – Each participating party/miner has access to the distributed database at all times without a central intermediary
- Shared and distributed ledger – The ledgers can be private, public, or semi-private / public. They can be shared among participants with privacy. The ledger entries are time-ordered and have cryptographical and computational architecture.
- Software development platform – Blockchain uses APIs. Peer-to-peer networks (P2P) in their software development platforms. Since the ledger is digital, intelligent and programmable contracts could be designed.
- Peer-to-peer network – Participating nodes communicate with each other directly without the need for a central node

- Cloud computing – Cloud computing platforms are used by Blockchains. They enable to use large amounts of resources for data storage and can bring flexible and scalable processing resources for data analysis.
- Wallet – A secured data storage location for user credentials like user ids, passwords, certificates, and encryption keys.

e. Types of Blockchain

- Blockchain technologies can be broadly classified into three types namely (Lin & Liao 2017):
- Public Blockchain: A public blockading is an open-ended permission-less network where anyone can participate without permission, execute consensus and maintain the shared ledger. Everybody can check and verify the transactions in a public Blockchain and can also participate in the consensus process. Examples are Bitcoin and Ethereum.
- Public Blockchain has the advantage of being more secure. The disadvantages are low privacy, less eco-friendly, and require huge computational power and energy ("How Blockchain Architecture Works?" 2018)
- Consortium Blockchain: This is a hybrid Blockchain which is partly private and partly public. The ability to read and write transactions is extended to some nodes which also controls the consensus process. This type of Blockchain exhibits properties of the node of authority can be chosen in advance, data can be open or private, has partnerships like business-to-business, and can be seen as partly decentralized. Examples are HyperLedger and R3CEV.
- Private Blockchain: Private Blockchain is permissioned networks which require an invitation to participate in the network. These networks put a restriction on entry of participants. It operates like a centralized database system that restricts access to users. Examples are Bankchain and Ripple.

f. Multi Cryptocurrency Payment Gateway

Cryptocurrency Payment gateway is a decentralized payment platform through which users can send and receive payments in multiple cryptocurrencies. The payment gateway reduces the number of intermediaries involved in a transaction. It also aims to increase the use of digital coins. Cryptocurrency payments made through these decentralized payment gateways are much more secure and are less vulnerable to malicious attacks. They also facilitate global transactions in multiple cryptocurrencies between suppliers, distributors, businesses, and customers at a lower cost. Besides payment transactions, some Blockchain-based payment gateways, such as ErosCoin gives a whole ecosystem. The payment gateways also aid in making smart contracts. In-chat payment feature and free peer-to-peer mass payments are other facilities from Eroscoin (Pauw 2017).

These Blockchain payment gateways, for instance, ErosCoin, accepts more than 500 types of cryptocurrencies. The other benefits of the gateway are convenience, speed, and cost-saving. The payments are completed in 15 to 20 seconds to anywhere in the world, as against 3 to 4 days taken by

a traditional payment gateway. The multi-cryptocurrency acceptance platform eliminates the need for separate applications for various cryptocurrencies (Pauw 2017).

g. Difference between Blockchains and Databases

In a traditional payment system for instance, in a merchant-bank transaction, the data on a payment is recorded in the bank as well as the merchant's database. The question that arises here is whether the Blockchains have similar or different databases. There are many types of traditional databases like relational databases, key-value stores, columnar databases, document databases, and graph databases. The databases can be centralized in a single location or can be distributed over many sites and connected by a computer network. The Blockchain concept is similar to the distributed database architecture. Distributed database partitions larger information retrieval and divides problems into smaller ones. A user is not aware of the database network topology or database distribution across various nodes. The connected nodes need not be homogenous in a distributed database (Peters & Panayi 2015).

In a distributed database, modifications done at one location are propagated to the various nodes through a "master-slave" approach. Updates to the master database are propagated to the slaves. There is one problem here when two copies of the data get modified by different write commands simultaneously. A Blockchain can be viewed as such a distributed database which can prevent such issues. A Blockchain network will reject a transaction from a node where the balance has already been spent by another node. This is one of the differences between databases and Blockchains.

Another difference is that Blockchains have the ability to create self-enforcing contracts. Each node can solve a large set of complex problems to add a block to the Blockchain and they themselves act as built-in virtual machines. The traditional databases are only data storage points and not smart contracts (Peters & Panayi 2015).

(iii) Cryptocurrency Transactions using Blockchain payment in E-commerce

Cryptocurrency adaption has made international transactions easier by minimizing the cost and processing time. To send or receive cryptocurrency, a cryptocurrency wallet is needed. There is also another option of using a Point-of-Sale (PoS) machine. The merchant account is integrated into the PoS. A cryptocurrency wallet is a software program that stores the public and private keys of users and interacts with various Blockchains to send or receive money. Unlike a traditional wallet, this digital does not store money but only the keys or addresses. When a person sends a digital currency, they are signing off ownership of the coins to the recipient's wallet's address. They send the funds to the recipient's public key address. To unlock the sent funds, the private key stored in the recipient's wallet must match with the public address sent by the recipient. If they match, the currency balance in the sender's wallet will decrease and that of the recipient will increase. There is no exchange of real coins. A transaction record or block is created in the Blockchain. Software wallets are desktop, online, and hardware ("Cryptocurrency Wallet Guide: A Step-By-Step Tutorial" 2018).

The steps of sending/receiving cryptocurrency are ("How to Send and Receive Cryptocurrency" 2018):

- The first step is to create a digital wallet.
- Add merchant's public key to the wallet.
- In the wallet, enter the public key of the merchant and the amount to be sent. PoS can be integrated into the merchant'
- At the receiving end, this public key will be matched with the merchant's private key. If they match, the transfer is made.

If the transfer is done in person, it can be done by scanning the QR code from the sender's mobile with the wallet of the receiver and the transaction is completed.

(iv) Pros and Cons of Using Blockchain as an Online Payment Source

E-Commerce would like to offer more payment options to customers to attract them to do business with them. The popularity of cryptocurrencies is making them acceptable as one of the payment source. Many market leaders have started to accept cryptocurrency as payment. Important among them are Microsoft, Sears, tesla, Shopify and PayPal. In Japan alone, it is estimated that over 250,000 businesses accept bitcoins (Vivo 2018). Cryptocurrencies have their own benefits and disadvantages.

Benefits: The benefits of using cryptocurrencies in business are many, some of which are defined hereunder ((Vivo 2018), (Abner 2015), and (Dumitrescu 2017)):

- Personal data protection – The chances of the retailer undergoing cyber-attack in a Blockchain transaction is very less and hence the risk of losing financial and personal data. The risk happens only when hackers get access to private keys.
- Lower transaction fees – The transaction fees of cryptocurrencies are lower than that of credit cards. Transaction $100 with a credit card would cost $3.37 whereas it would cost only $0.61 in a Blockchain transaction for the same value, meaning that credit card is 5.5 times costlier. In these transactions, the speed at which users receive money depends on the fees paid. Since the processing power is distributed across the network, the owners make money by charging fees from users to allow their transactions.
- Faster processing time – The transactions can take place near-instant speed and hence there is less waiting time between sales and payment clearance
- PCI compliance is not required as businesses do not carry the costs or responsibilities that come with processing sensitive information from customers like credit cards
- The transparency of transaction activities eliminates the need for businesses to produce documents about activities
- Protection from chargeback fraud – Chargeback fraud occurs when a customer makes an online purchase with a credit back, and then requests the issuing bank for a chargeback after receiving

the goods. In a traditional payment, since it takes 2-3 days for the payment to go to the merchant, the payment does not reach him for the goods purchased due to chargeback request from the customer. This type of fraud cannot happen with Blockchain payments as the payment is made immediately.

- Immune to inflation – The monetary inflation of cryptocurrencies has been steadily decreasing and will stop when it reaches its maximum limit of 21 million coins
- Increase in new customer traffic – Customers who want to experiment with cryptocurrencies will want to shop with it
- More repeat customers – Due to the conveniences it offers, the crypto payments will attract more customers
- Cryptocurrencies have gained legitimacy on wall-street due to investments from major organizations into it like Fortress Investment Group, New York Stock Exchange, and Pantera and Goldman Sachs.

Disadvantages: The disadvantages of cryptocurrencies and Blockchains are defined here ((Abner 2015), and (Dumitrescu 2017)):

- Volatile market – Cryptocurrencies market is very volatile and it can go up and down within a few hours. Transactions have to be only when their value increases to avoid losses.
- Poor security – Cryptocurrency programmers are not security experts but are from finance and development background. They need a different skill to understand hackers and hence security risks arise. Poor security leads to losing files and losing money from the entire wallet.
- Lack of solid anonymity – The Blockchain transactions and centralized services like wallets and exchanges are not completely anonymous. Using statistical techniques and pattern analysis, the profiles of at least 60 percent of Blockchain users can be revealed.
- Prone to scams – The private key gives access to the wallet to the owner. If it is lost, even the owner cannot open it. Many scams amounting to over 10 million dollars have been reported with cryptocurrency transaction between 2011 and 2014 like high-yield investment programs like Ponzi schemes, mining investment scams, deposits in “scam wallets”, and exchange scams.
- New cryptocurrencies can obsolete older ones – New cryptocurrencies are being constantly developed and they come with new technologies and improvements. Bigger players like master cards have plans of introducing cryptocurrencies and when they do so, they will come with a bigger network and improved technology. This leads to a lower market capitalization for other competitors.
- Trust as a saving point – People, especially the older generation, are reluctant to use cryptocurrencies as a saving. The computations and complex algorithms also make it difficult for the people to understand its working and hence they are reluctant to use this as a savings option.

Many of the Blockchain features match the needs of online payment infrastructure namely (Kulkarni, 2017):

- Security – Distributed processing prevents manipulation of records, thereby preventing fraud and security breach
- Processing Speed – Distributed ledger helps to connect all parties for faster processing of payment
- Traceability
- Global registry in public ledger

Benefits of using Blockchain technology in online payments are ("Know more about Blockchain: Overview, Technology, Application Areas and Use Cases" 2018):

- Each and every record in a Blockchain is validated and hence payment is secure and reliable
- All the transactions are authorized by miners and hence they are immutable and are prevented from hacking
- No central authority is needed for Blockchain peer-to-peer transactions
- Decentralized technology and hence is independent of government regulations, making it more flexible.
- Challenges in adopting Blockchain technology for online payments are ("Know more about Blockchain: Overview, Technology, Application Areas and Use Cases" 2018) and (Daisyme 2018):
- High technology standards – High standards are needed for security, robustness, and performance of Blockchains
- Upgrading regulations and legislations – New legislations have to be defined to integrate Blockchains into the financial market infrastructure
- Managing operational risk – Operational risk should be minimized when moving to the new payment system, which will also require that the traditional system is set up as the fallback system
- The complexity of technology – Unable for the average person to understand
- Huge network size – Hundreds and thousands of nodes are required for Blockchains to work in unison. This makes these systems vulnerable to attack and corruption.

B. Related Work:

(i) Major Security Issues in Using Blockchain for Online Payment

a. Security Risks:

Security risks that can arise in using Blockchain for online payment (Vyas & Lunagaria 2014) and ("Distributed Ledger Technology in Payment, Clearing and Settlement" 2017) are:

- Resilience and reliability – Multiple nodes are provided to provide reliability and continuous operation. However, this can also provide additional entry points for malicious actors who can compromise the integrity and confidentiality of the ledger.
- Continuous technological advancements can render the current cryptographic tools obsolete and ineffective. Integration of distributed ledgers into existing infrastructure can also lead to security breaches and threats.
- Should be operationally scalable depending upon requirements
- Legal framework need not provide settlement finality always
- Distributed ledgers pose legal risks if a settlement's arrangement is ambiguous
- Timejacking attacks when the attacker posts inaccurate timestamp on a block
- Online wallets are more prone to Distributed Denial-of-Service (DDoS) attacks
- ">50%" attack when a miner or group of users acquire more than 50% of computing power and can self-reverse transactions
- Double spending when the attacker makes more than one transaction using a single coin
- Selfish mining where a group of users can obtain revenue more than their mining power.

b. Security Threats:

As with the other payment methods, Blockchain payment systems also have security threats and concerns. The security issues are briefed as under ((Vyas & Lunagaria 2014) and (Lin & Liao 2017)):

- Attacks on Wallet Software - Wallets are used by cryptocurrency customers to manage the currencies owned by them. Online wallets are more vulnerable to security attacks than offline wallets. Hence they need to be encrypted and backed up off-line. Distributed Denial of Service (DDoS) attacks are potential threats for online wallets.
- Time jacking attacks – The time counter of a node in the network is altered by the attacker and this deceived node may accept an alternate blockchain. The consequences are double-spending and waste of computational resources.
- ">50%" Attack – This is one of the major threats to a Blockchain network and happens when a user or group of users get hold of more than 50 percent of computing power in mining. They do this by getting hold of the "nonce" value in a block. They can then execute, modify, and self-reverse transactions and prevent the mining of valid blocks.
- Double-spending – Double spending attack is one where an attacker makes more than one transaction with the same coin, resulting in invalidation of the "honest" transaction and validating the "fraud" transaction. An attacker makes a transaction with a coin and simultaneously, another transaction with the same coin is done to another address. By varying the timestamp, the second fraud transaction can be made as a real one. Blockchain peers will not accept two transactions with the same input. They will validate only the first one reaching them and hence the fraud transaction will be validated and the original one will not be confirmed.

- Selfish mining – It allows a pool of sufficient size to obtain revenue larger than its mining power. The attacking miners will force honest miners to perform wasted computations. The selfish miner will keep their blocks private, will secretly bifurcate their Blockchain and earn more revenue.
- Fork Problems – Fork problem is related to decentralized node version agreement when the software upgrades. This is an important problem as it involves a wide range of Blockchain. When a new version of Blockchain software is incorporated, consensus rule in nodes also changes. So there are new nodes as well as old nodes in a Blockchain network. Problems arise in getting consensus between old nodes and new nodes during transactions between them. The agreement or consensus between old and new nodes is not compatible.

  Hard fork problem occurs when the old node verification requirement is stricter than the new node. Soft fork problem occurs when the new node verification requirement is stricter than the old node. Besides these, there are many other security threats. A summary of the security threats, the location of their attack or the vectors, and the reason because of which that attack could occur are represented in the table shown in Table 1.

Table 1: Taxonomy of Blockchain Security Threats (Mosakheil 2018).

Security Threats	**Attack Vectors**	**Cause**
Double-Spending Threats	Race Attack	Transaction Verification Mechanism
	Finney Attack	Transaction Verification Mechanism
	Vector 76 Attack	Transaction Verification Mechanism
	Alternative History Attack	Transaction Verification Mechanism
	51% Attack	Consensus Mechanism
Mining/Pool Threats	Selfish Mining/Block-discard Attack	Consensus Mechanism
	Block-Withholding Attack (BWH)	Consensus Mechanism
	Fork-After-Withhold Attack (FAW)	Consensus Mechanism
	Bribery Attack	Consensus Mechanism
	Pool Hopping Attack	Consensus Mechanism
Wallet Threats	Vulnerable Signature	ECDSA flaws - Poor randomness
	Lack of control in address creation	Public nature of the blockchain
	Collison & Pre-Image Attack	Flaws in ECDSA, SHA256 & RIPEMD 160
	Flawed Key Generation	Flaws in implementing ECDSA
	Bugs & Malware	Client design flaws
Network Threats	DDoS Attack	External resources, contracts under-priced operations
	Transaction Malleability Attack	Flaws in blockchain protocols - Transaction ID
	Timejacking Attack	Flaws in blockchain protocols - timestamp handling
	Partition Routing Attack	Flaws in Internet routing - routing manipulations
	Delay Routing Attack	Flaws in Internet routing - routing manipulations
	Sybil Attack	Structured P2P network limitation - forge identities
	Eclipse Attack	Flaws in blockchain protocols - outgoing connections
	Refund Attack	Flaws in BIP70 payment protocol - Bitcoin refund

		policy
	Balance Attack	Consensus Mechanism
	Punitive and Feather Forking Attack	Consensus Mechanism - blacklisting transactions
Smart Contacts Threats	Vulnerabilities in contracts source code	Program design flaws
	Vulnerabilities in EVM Bytecode	EVM design flaws
	Vulnerabilities in Blockchain	Program design flaws
	Eclipse Attack on Smart contact blockchain	EVM design flaws
	Low - level attacks	underprice operations

(ii) Existing Solutions for Blockchain-based Payment Systems

Existing resolutions for security issues identified in the earlier section are discussed briefly in this section. The recently developed solutions will be discussed.

a. Attack on Wallet Software

A wallet stores the digital credentials of cryptocurrency holdings and allows the user to access and spend them. Software wallet attacks can be in the form of loss of private keys or signature forgeries leading to loss of digital money. Barber et al. (2012) propose the idea of "Super-Wallet" to address the user concern which is split across multiple computing devices. The super-wallet acts as the user's "personal bank" where most of the user's coins are stored. Besides this, the user also carries a sub-wallet in the smartphone. User can withdraw small amounts of money from super-wallet into sub-wallet whenever needed. User can spend money from the smartphone itself and need not go to super-wallet. Even if a smartphone is lost or attacked by malware, only a small amount of money will be lost. The larger amount is still secure in super-wallet and can be spent through a multitude of devices. Constant backup of wallet file helps to overcome accidental loss or data destruction. Wallet backup is done similar to other cryptographic assets due to the secrecy. It is also complex due to the continual creation of keys. Another way of protecting a wallet is to encrypt it using a strong password and replicating the resultant ciphertext. Password-based encryption can be online, offline, or trusted paths (Barber et al. 2012).

b. Time jacking attacks

The network time is used to validate new blocks to the Blockchain. An attacker announces inaccurate time stamps and alters a node's time counter and deceives it to accept a block from another Blockchain instead of a block from its own network. This attack is a theoretical vulnerability. This issue could be overcome by defining acceptable timestamp ranges based on previous block timestamps. Other solutions are (Boverman 2011):

- Using the node's system time for timestamps instead of network time,
- Maximum initial attack window is between 70 and 140 minutes. This is shortened to 30 to 60 minutes, thereby restricting the networks node time to within 30 minutes. This method cannot entirely reduce attacks but can reduce them.

- Blocking untrusted peers and having a secure node can reduce the extent of attack but will not resolve the global time agreement problem
- Increasing confirmations before accepting a transaction

c. >50% attacks

51% attack is an attack on the Blockchain network by a group of miners controlling more than 50% of a network's mining hash rate. Such an attack is hypothetical and has not known to have occurred. There is a possibility of such attacks happening in the future even with less than 50 % computing power ((Vyas & Lunagaria 2014).

d. Double spending

Double spending is signing over the same coin to two users. It is the highest occurring attack in cryptocurrencies. To prevent double-spending of the same coin, Cryptocurrencies rely on a hash-based Proof-of-Work (PoW) scheme where users are prevented from double-spending through a distributed time-stamping method. Even otherwise, double spending occurs mostly in fast payment scenarios where payment is done within 30 seconds, whereas it takes nearly 10 minutes to verify a cryptocurrency transaction (Karame et al. 2012).

Karame et al. discuss three methods of detecting double-spending in cryptocurrencies namely (1) Using a "Listening" period, (2) Inserting observers in the network, and (3) Forwarding double-spending attempts in the network.

In the first method, a "listening" period of a few seconds is employed to detect double-spending of coins before delivering them. Since every transaction takes a few seconds to propagate to every node in the network, the network checks if any node attempts to double-spend the coin that was previously received. The second method is to insert an observer node which would directly relay all transactions that are received by the nodes. The third method proposes that cryptocurrency peers forward all transactions that try to double-spend the same coins in the network.

e. Selfish mining

Selfish mining is possible for any conniving group of miners. Currently, the threshold at which selfish mining is effective is close to zero. The cryptocurrency network is modified using a backward-compatible protocol, to raise this threshold limit to ¼, so that when all non-selfish miners adopt it, it will benefit them (Eyal & Sirer 2013).

f. Fork problems

Forking is duplication of a Blockchain history when there is a conflict between rules of old and new nodes. The nodes of a Blockchain have been programmed to follow that Blockchain whose proof-of-work difficulty is the largest. It discards blocks from other forks. The discarded blocks are called orphan blocks. This problem is resolved by collecting transactions on the discarded branches into blocks in the existing branches (Barber et al. 2012).

Table 2: Classification of Attacks on Bitcoin (CryptoBullsAdm 2018).

Possible attacks on Bitcoin			Probability of such attack in the next 10 years	Possible damage if the attack was successful	Probability X damage
Attacks to slowdown the Bitcoin adoption	**Legal Attacks**	Ban of Bitcoin by a small country	High	low	medium
		Legal persecution of a major Bitcoin merchant	High	low	medium
		Public persecution of a prominent Bitcoin figure	High	low	medium
		Oppressive taxation of Bitcoin by a major power	Medium	medium	medium
		A UN/WTO-level legal attack on Bitcoin	Low	high	medium
		Ban of Bitcoin by several major powers(US, EU, China)	Low	medium	medium
	Cyberwarfare	Large-scale attack on Bitcoin merchants	Medium	medium	medium
		Hack of a major Bitcoin merchant	High	low	medium
		Mass digital surveillance to steal private keys/ de-anonymize users	Medium	high	high
		Large-scale attack targeting Bitcoin users	Medium	medium	medium
	PR attacks	Influencing the public opinion to associate Bitcoin with crime(drugs etc.)	High	low	medium
		Spreading FUD about Bitcoin in the media	High	low	medium
		large-scale leak of user information from a major Bitcoin merchant	High	low	medium
	Financial attacks	Creation of a competing state-supported crypto	Medium	medium	medium
		Pumping funds into a competing centralized crypto o make it the biggest	High	medium	high
		Large-scale market manipulation to spread FUD about Bitcoin	High	medium	medium
		Creating a similarity named altcoin to confuse users	High	low	medium
	Hybrid attacks	astroturfing social and political opposition to Bitcoin (r/buttcoin etc.)	High	low	medium
		Gaining control over a major Bitcoin community	Medium	medium	medium
		Splitting up a major Bitcoin community	High	low	medium
Attacks to reduce the efficiency of the Bitcoin infrastructure	**Cyberwarfare**	Creating a flood of transactions with the goal of slowing down the network	High	medium	medium
		Sybll attack on nodes	high	low	medium
		DoS attacks on nodes	high	low	medium
		Timejacking of nodes	high	low	medium
		A majority attack by state-sponsored miners	medium	medium	medium
		Using some zero-day exploit of the client code to disturb the network	low	high	medium
		Using some zero-day exploit in the Bitcoin-related cryptography	low	high	medium
		Malicious modification of transactions on the Internet Backbone level	low	high	medium
		Compromising the code with a carefully designed hidden vulnerability	low	high	medium
	Hybrid attacks	A country-wide filtering of Bitcoin traffic	medium	high	high
		Forcing a major CPU or OS provider to implement relevant vulnerabilities	medium	high	high
		Forcing a major soft-/hardware wallet provider to implement vulnerabilities	medium	medium	medium
		Gaining direct control over a major soft-/hardware provider	medium	medium	medium
Attacks to slowdown the bitcoin development	**Hybrid attacks**	Gaining direct control over a major miner by a state-sponsored entity	high	medium	high
		Preventing necessary upgrades from being implemented	high	medium	high
		Manipulating a part of the community into supporting a malicious fork	high	medium	high
		Gaining direct control over an influential dev	medium	medium	medium
		Hijacking admin rights in a major code repository	low	low	low
		Killing or incapacitating an influential dev	low	low	low

(iii) Classification of Blockchain Attacks

The Blockchain attacks can be of many types – legal, financial, cyber warfare, PR attacks to spoil the good name, and hybrid attacks. They are employed to slow down cryptocurrency development, adoption by businesses and common use, and to reduce the infrastructure. A tabulation of the attacks is shown in Table 2. Though it shows the currency like Bitcoin, the attacks are applicable to any cryptocurrency (CryptoBullsAdm 2018).

(iv) Cryptocurrency Policies and Regulations to make Online Payments

Money transactions are regulated by individual governments, banking authorities, and international bodies to maintain validity and prevent frauds and scams. Since cryptocurrencies are also a form of currency, but digital, they also have to undergo a similar procedure. The efforts on regulation, the involved bodies and the extent to which they have been able to govern and regulate cryptocurrencies are discussed in this section (Jaag & Bach 2016).

- Cryptocurrencies are hard for the government as they do not have any central point of access making it difficult for law enforcement. Since the system is anonymous, money holdings cannot be seized. Accounts cannot be frozen in the decentralized systems as in traditional banking systems.
- Due to their decentralized nature, the transactions can be done across borders. Hence regulations have to be coordinated across countries.
- Institutions and companies offering services related to cryptocurrencies can be regulated as they have a central point of access. For example, currency exchanges that act as a payment gateway between traditional currencies and cryptocurrencies can be forced to abide by regulations like anti-money-laundering law.
- The first guidance related to the regulation of these digital money services was issued by the Financial Crimes Enforcement Network (FinCEN) in the USA in March 2013. Individuals who use cryptocurrencies to sell and purchase goods do not fall under FinCEN but only businesses like cryptocurrency exchanges. Miners and software providers do not fall under this regulation.
- Business license of cryptocurrency activities was issued by New York State Department of Financial Services in August 2015. Several Bitcoin companies stopped their businesses due to these regulations.

(v) Abuses of Blockchain Technology

Blockchain technology is decentralized, anonymous, and distributed, and is termed as safe from hacking. But loopholes have been found and this technology has also been abused. Some of the abuses on Blockchain technology is discussed in this section.

a. Links to child abuse contents

German researchers found that anonymous persons are using bitcoin's blockchain to store and link to child abuse images. Besides storing financial data, Blockchains can also be used to store links and files. 59 files were found to contain images or links to child abuse. Spending Blockchain may not require a copy of Blockchain but mining techniques require that it be downloaded. 112 countries trading with cryptocurrencies consider possessing such contents as illegal (Claburn 2018).

b. Sex, drugs, and related illegal activities

The anonymity provided by cryptocurrencies has led to its use in the illegal trade of drugs, hacks and thefts, illegal pornography, and even murder-for-hire. There is also the potential to fund terrorism, launder money, and avoid controls. Cryptocurrencies have facilitated the growth of "darknet" online market places. FBI recently seized $4 million bitcoins from one such marketplace named "Silk road", explaining the enormity of the problem. "Silk Road" was found to conduct business mostly in drugs and weapons (Foley et al. 2018).

c. Tax evasion

Due to the anonymous nature of cryptocurrencies, there is the possibility of tax evasion. Some users have also reported the theft of their cryptocurrencies. Major retailers like Microsoft and Dell are accepting Bitcoin currencies. Bitcoin is used by many parties and its wide use has eliminated its need to get converted into traditional currency by intermediaries or exchanges and integrates it with the real economy. This lack of intermediaries also helps in tax evasion since the US employs only intermediary-based tax-enforcement mechanisms (Ruppert 2017).

d. Money laundering

Cryptocurrencies present the risk of money laundering. They are not linked to a person's identity and only depend on the private key to connect to the wallet or account. There is also no central record-keeping which financial institutions can check. Individuals also need not have to rely on intermediaries for money transfers. All these give advantage to people to transfer a large amount of money to anonymous accounts (Sharma 2018).

e. Terrorism

Terrorists evolve tactics to adapt and break the barriers imposed on their activities by security and intelligence forces. They always need funds to support their activities. The volatility and anonymity of cryptocurrencies have made it be used to fund terrorists. In June 2016, the online propaganda forum of Salafi Jihadist Group Mujahedeen Shura Council, a terrorist group, added the option of donating in "Bitcoin" in its campaign. This showed that the terrorist group is well equipped to receive cryptocurrencies, convert it to fiat currencies, and use it for buying and selling. Terrorist groups are only at the infant stage of receiving cryptocurrency payment but this should be curbed at the initial stage itself (Thein 2017).

3. Research Methodology

Research methodology lays out the systematic plan to conduct research. It describes how the sample, measures, and analysis work together to attain the research objectives. This section explains the method by which research is carried out, the source of research data, data collection methods, and data analysis methods. This research provides an understanding of the application of cryptocurrencies in E-commerce online payment. It proposes to attain this in two parts namely:

A. Qualitative and Quantitative research:

The responses of the general public will be collected through a questionnaire on their understanding of cryptocurrencies, the associated risks on security and privacy, and their view of cryptocurrencies as an investment option. The responses are analyzed quantitatively to find if cryptocurrencies are being favored as secure payment and investment choice. The security and privacy issues expressed by the public will be studied qualitatively to find resolutions to overcome them from existing literature. The concerns expressed by the general public on making cryptocurrencies as an investment option are qualitatively analyzed and resolutions are found from literature to address them.

(i) Qualitative Method

Qualitative data refers to texts, words, and sounds collected from users or from literature. In this research, data responses from cryptocurrency users are only numerical in nature and no textual data is collected. Similarly, the secondary literature analysis is conducted on pre-defined subjects like security issues in cryptocurrency usage and abuses of Blockchain technology. Hence the qualitative method of data collection is not employed in this research. However, secondary data are qualitatively analyzed to substantiate and counter user responses and to provide responses for research questions on security issues and abuses of Blockchain technology.

(ii) Quantitative Method

Quantitative data deals with measurable numbers, quantities, and values and are expressed in numerical form. The questionnaire responses are recorded in numerical values. These responses are analyzed using existing literature to arrive at meaningful interpretations and results. The purpose of this research is also to identify trends in the problems faced by cryptocurrency users, who may be new or experienced users.

B. Data Collection Methods

Data collection is the process of gathering data on variables of study in a systematic method to answer defined research questions. Data collection falls into two categories namely primary data and secondary data. Primary data are original in nature and are collected for the first time. Primary data is collected through instruments like surveys, questionnaires, telephone, mail, and direct interviews where responses of participants are recorded, characterized and analyzed. Secondary data is the data collected from previously publishes sources like books, journals, online portals, and others (“Data Collection” 2017). This research involves the collection of both primary and secondary data.

Primary data collection can be quantitative or qualitative. Quantitative methods are based on calculations with inputs from closed-ended questions. Qualitative research methods are not based on mathematical calculations but are associated with words, sounds, emotions, and other non-quantifiable elements ("Data Collection" 2017). The data collection method for this research is based on a closed-ended questionnaire where responses will be collected in numbers. The questionnaire will also invite comments from the respondents which are qualitative in nature. Hence both qualitative and quantitative research methods will be employed for this work.

Besides the questionnaire, this research work also employs secondary data collection in the form of literature, books, journals, and other sources. This literature is on recommendations for using Blockchain as an online payment medium, and resolutions to overcome security issues due to Blockchain payments and attacks. Literature is also collected pertaining to the Blockchain technology itself on improving its application as a payment medium, risks, and opportunities for systems using Blockchain technology, and preventing abuses on the Blockchain technology.

(i) Primary Data – Questionnaire

Primary data will be collected through a questionnaire. Sample population that has an understanding of cryptocurrencies is selected to give responses to the questions. The sample size would be 100 numbers.

The questionnaire has questions on the users' willingness to adopt cryptocurrencies as a payment medium and investment, and their opinion on threats to cryptocurrencies. It has 15 questions. The questionnaire is shown in appendix A. The variables in the questionnaire can be independent or dependent. Since the data are dependent upon users' response, they are dependent variables.

The variables employed to collect data in the questionnaire are of different types like binary, nominal, ordinal, interval, and ratios. Binary, nominal, and ordinal variables are called categorical variables ("Types of Variables – Categorical" 2017). A binary variable has two mutually exclusive Choices. When the variable has more than two choices to select from, it is called a nominal variable. A variable that has categories which can be put in a logical order is called as an ordinal variable. Interval and ratios are called continuous variables ("Types of Variables – Continuous" 2017). Interval variable is one where the variable choices are ordered and the level between each category is equal and static. Ratio variable is similar to the interval but has a clear "0" point and the differences between them are comparable.

(ii) Secondary Data

Secondary data is collected from storage sources that may or may not be published. The data should be reliable, suitable, and adequate. Secondary data is used in this research for two purposes.

For the first purpose of qualitatively analyzing the questionnaire responses, secondary data from journals, books, web material, public records, and many other sources are used. Primary data is the key resource for this research and secondary data is used as supplementary wherever necessary ("Methods of data collection – Primary and Secondary data" 2016).

The second purpose of employing secondary data is to undertake a theoretical study on resolutions for (1) security problems in using Blockchains as payment source in e-commerce applications (2) attacks on Blockchain networks and (3) abuses of Blockchain technology. This part is not on problems faced on users but focusses on existing resolutions available to overcome these problems.

C. Research Sample

This research focusses on issues with cryptocurrencies and corresponding resolutions and hence people who have knowledge on cryptocurrencies will be suitable to answer the questionnaire. The sample population is selected with great care. The respondents should have some basic knowledge about cryptocurrencies, Blockchains, their applications, security issues, and the future potential of cryptocurrencies. Blockchains are ledgers that record cryptocurrency transactions. Common users are not aware of what goes in Blockchains. Hence questions on Blockchains are not included in the questionnaire. People in the age group of 25 to 40 years will be more interested in learning and experimenting with the latest technologies and applications. Hence, people who are familiar with cryptocurrencies and in the age group of 25 to 40 years, from various professions, are selected for administering the questionnaire. The sample size is 20 to 25 numbers is considered as appropriate to get enough data for qualitative and quantitative analysis.

D. Data Analysis

The process of extracting relevant information from the collected data is called data analysis. Data analysis identifies common patterns in data responses and critically analyses them to attain research objectives. The questionnaire responses are quantitatively analyzed. Secondary literature is qualitatively analyzed to critique questionnaire responses and provide resolutions for cryptocurrency security issues, attacks, and abuses.

Quantitative data analysis is the process of converting data into numerical forms and analyzes them for making interpretations. Each question and its responses are analyzed individually to infer results from the numerical responses. Theoretical literature is also used to substantiate the interpretations. No explicit statistical tools are needed for this data analysis.

Qualitative data are non-numerical in form. Qualitative data analysis is not performed on primary data in this research. It is basically opinions and resolutions from existing secondary literature on issues identified from user responses in questionnaire and research objectives. This is essentially the procedure of document studies, where documents are studied to understand issues and resolutions to these issues.

The security and privacy issues expressed by the public will be studied qualitatively to find resolutions to overcome them from existing literature. The concerns expressed by the general public on making cryptocurrencies as an investment option are qualitatively analyzed and resolutions are found from literature to address them. Besides resolutions for research questions are also found out.

E. Ethical Considerations

In this research on cryptocurrencies, a few practices were followed keeping in mind the end goal to not disregard the moral practices of research. They are:

- Participants of the research are people familiar with cryptocurrencies
- Full assent ought to be gotten from the exploration members who take up the questionnaire
- Research scope ought to be straightforward to the members and research subtle elements ought to be clearly conveyed to them
- Research questions should be relevant to the participant's field and knowledge as well as with the scope of research (only cryptocurrencies and Blockchains)
- The privacy rights of the participants should be protected
- Research information from members relates to this research only
- Research data are confidential and should be protected from manipulation
- Participants ought to be treated with pride and regard
- They should have enough time to understand and answer the questionnaire
- Literature used should be original contents and from authenticated resources
- All sources used in this research are properly referenced to keep away from plagiarism

4. Research Findings

A. Results of Data Analysis:

The data analysis involves two parts – (1) analyzing responses from the questionnaire and finding resolutions for problems reported and (2) finding resolutions for security issues and Blockchain abuses that were identified in the literature review, from secondary literature. The second part is addressed by presenting resolutions from relevant literature on the identified issues whereas the first part works on questionnaire responses. The outcome of the questionnaire responses is briefed out in this sub-section.

The questionnaire was on the practical use of cryptocurrencies, common people's familiarity with them, their concerns about the digital currency, and their opinion on using it as an investment option. The responses were collected from 100 professionals across multiple occupations who are in the age group of 15 to 40 years. The questionnaire consisted of 15 closed-end questions where the respondent records his / her option by selecting one or multiple choices. There are no open-ended questions that invite open responses. Based on the recorded responses, the issues faced by the common public are identified, and their possible resolutions are studied from secondary literature.

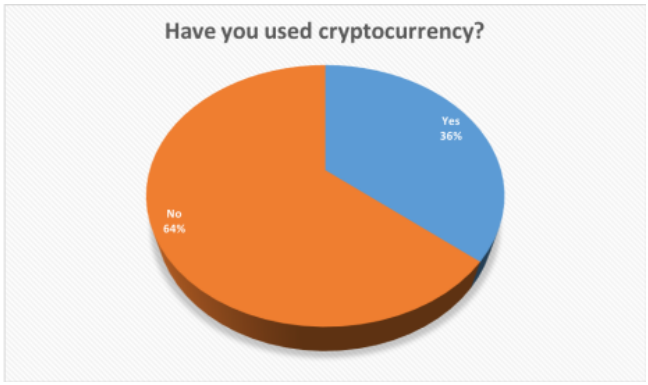
The collected responses show that the majority of the population is aware of cryptocurrencies but only one-third of them have actually used them. 58 percent of the respondents would like to try out the digital currencies but their main reason is to know what it actually is and not because they are confident to use it. More than 70 percent of them have said that they know that cryptocurrencies can

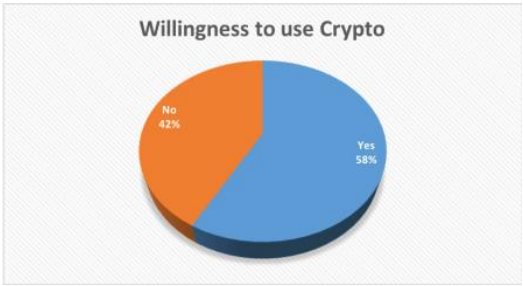
be used for online shopping and bill payments, but the only lesser population is aware of other applications. Most of them are hesitant to use cryptocurrencies due to poor security, and lack of data protection is their chief concern in terms of security.

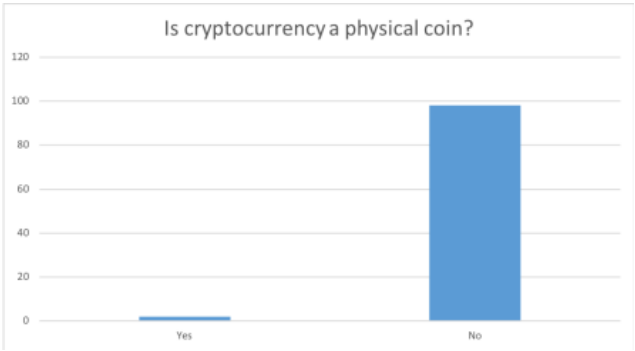
The respondents are skeptical about cryptocurrencies having a long-term future. Nearly 80 percent of them do not consider cryptocurrencies as an investment option and also would not like to invest in ICO (Initial Coin Offering) from a company. ICO is a process where companies sell their crypto tokens in exchange for bitcoin and ethereum to raise funds. Even if the digital currencies are comparable with gold, they are not willing to invest in cryptocurrencies in the present. They are afraid that cryptocurrencies do not have future, are subject to scams, and illegitimate. These threats and potential resolutions are also studied using literature in the next chapter. Resolutions for questionnaire responses are analyzed and discussed in detail.

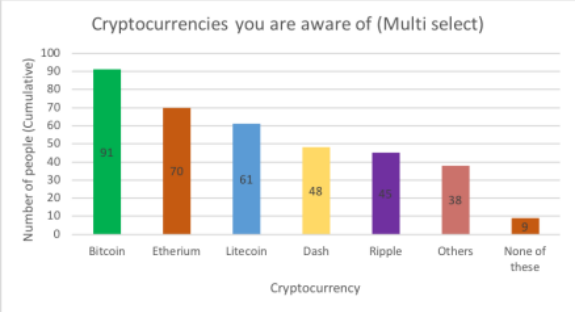
B. Analysis and Discussion of Questionnaire Responses:

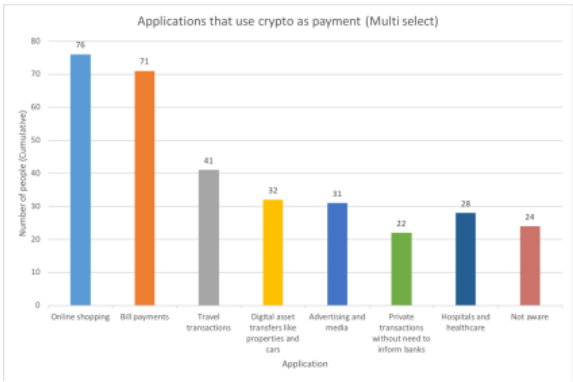
The questionnaire on cryptocurrencies has questions on cryptocurrencies related to respondents' awareness of cryptocurrencies, their applications, their concerns on security, and their opinion on using the digital currencies as an investment option. There are 15 questions answered by 100 respondents. The questions are of multiple-choice type. Depending on the question, one or more options can be selected as answers. Each of the questions is quantitatively analyzed in this section. The responses are critically studied and analyzed, wherever necessary with secondary literature and are shown in Figure 1.

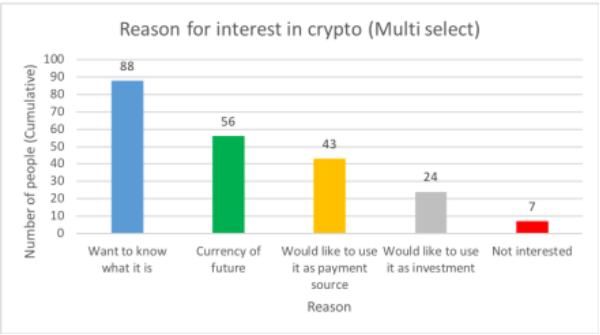


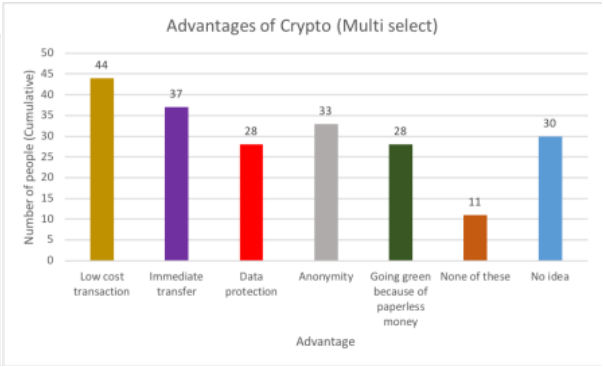


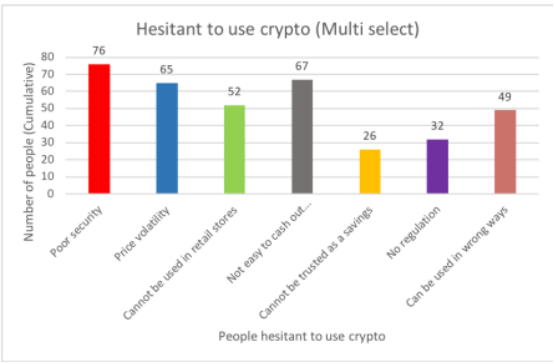


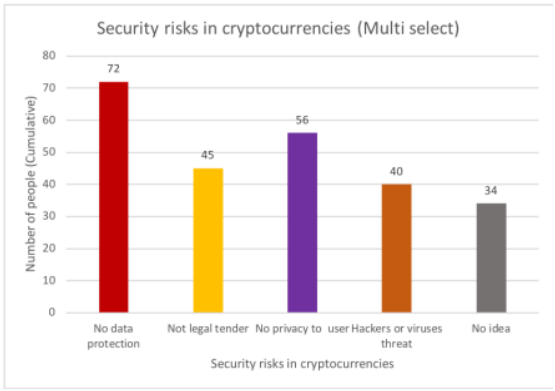

Cryptocurrencies you are aware of (Multi select)
Number of people (Cumulative)
Bitcoin
Etherium
Litecoin
Dash
Ripple
Others
None of these
91
70
61
48
45
38
9
Cryptocurrency

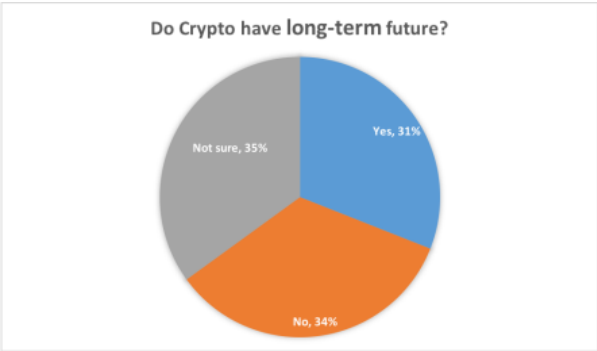

Applications that use crypto as payment (Multi select)
Number of people (Cumulative)
Online shopping
Bill payments
Travel transactions
Digital asset transfers like properties and cars
Advertising and media
Private transactions without need to inform banks
Hospitals and healthcare
Not aware
76
71
41
32
31
22
28
24
Application

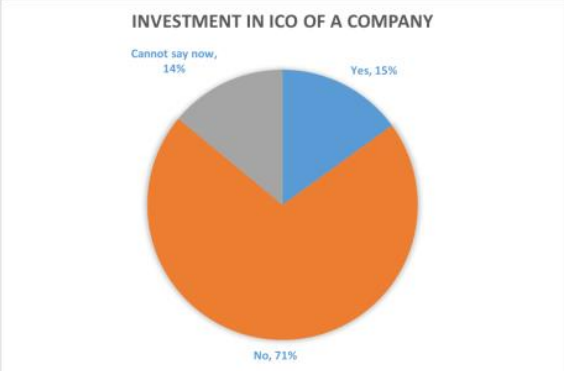

Reason for interest in crypto (Multi select)
Number of people (Cumulative)
Want to know what it is
Currency of future
Would like to use it as payment source
Would like to use it as investment
Not interested
88
56
43
24
7
Reason


Advantages of Crypto (Multi select)
Number of people (Cumulative)
Low cost transaction
Immediate transfer
Data protection
Anonymity
Going green because of paperless money
None of these
No idea
44
37
28
33
28
11
30
Advantage


Hesitant to use crypto (Multi select)
Number of people (Cumulative)
Poor security
Price volatility
Cannot be used in retail stores
Not easy to cash out...
Cannot be trusted as a savings
No regulation
Can be used in wrong ways
76
65
52
67
26
32
49
People hesitant to use crypto


Security risks in cryptocurrencies (Multi select)
Number of people (Cumulative)
No data protection
Not legal tender
No privacy to user
Hackers or viruses threat
No idea
72
45
56
40
34
Security risks in cryptocurrencies


Do Crypto have long-term future?
Yes, 31%
Not sure, 35%
No, 34%


INVESTMENT IN ICO OF A COMPANY
Cannot say now, 14%
Yes, 15%
No, 71%

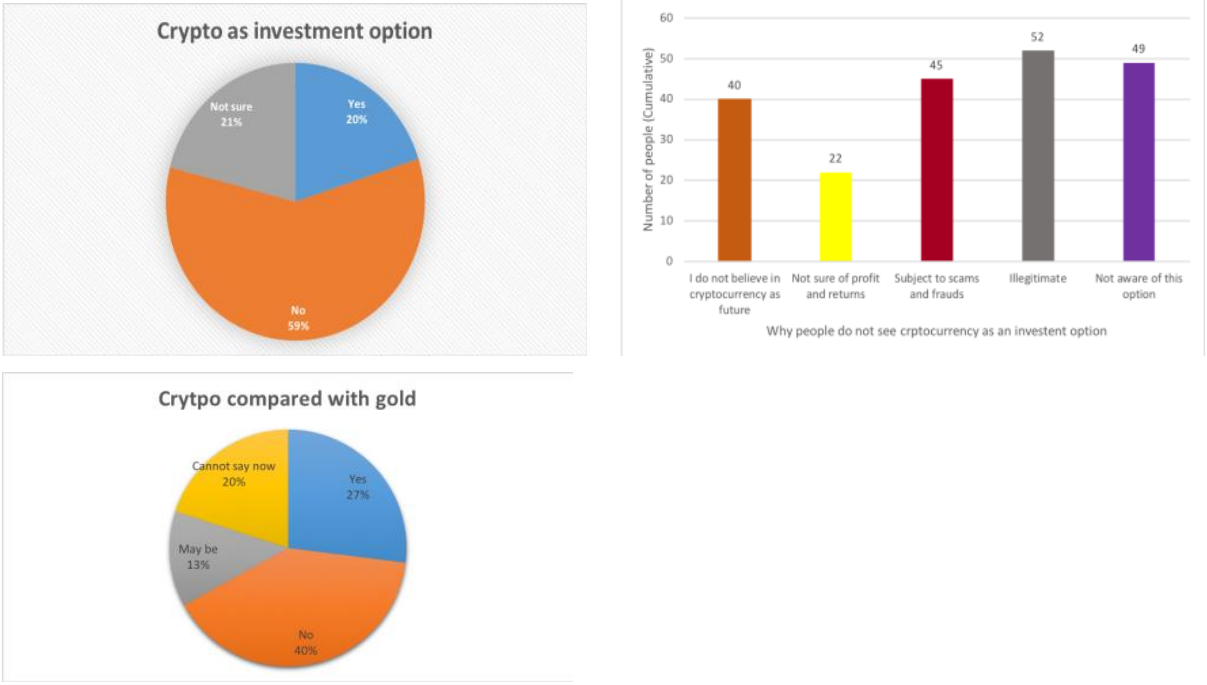


Figure 1: Questionnaire responses (left-to-right, top-to-bottom) on (i) awareness of cryptocurrencies, (ii) Have you used cryptocurrency?, (iii) Are you willing to use cryptocurrency? (iv) Is cryptocurrency a physical coin?, (v) What are the cryptocurrencies you are aware of?, (vi) Do you know about the applications where cryptocurrencies can be used as payment?, (vii) What makes you take an interest in cryptocurrency?, (viii) What do you think are the advantages of cryptocurrencies?, (ix) Why are you hesitant to use cryptocurrency?, (x) What do you feel are the security risks in cryptocurrencies?, (xi) Do you think cryptocurrencies have long-term future?, (xii) Will you invest in ICO from a company?, (xiii) Do you consider cryptocurrencies as an investment option?, (xiv) Why do you not see cryptocurrency as an investment option?, and (xv) Cryptocurrencies are more or less compared with gold rather than with money or stock exchange. If it is in par with gold, will you invest in it?

Below is a list of the questions asked to the participants along with their responses.

Question 1: Are you aware of cryptocurrencies? (1) Yes and (2) No

Response: Response shows that 96 percent of them are aware of cryptocurrencies. This makes the sample population a proper fit to answer rest of the questions.

Question 2: Have you used cryptocurrency? (1) Yes and (2) No

Response: Response shows that only 36 percent or about 1/3rd of the sample population have used cryptocurrency. This shows that the currency has not made a good entry into people's desks.

Question 3: Are you willing to use cryptocurrency? (1) Yes and (2) No

Response: 58 percent have expressed their willingness to use cryptocurrencies, which is a positive sign. This is 22 percent in addition to those who have used cryptocurrency and hence will be new users.

Question 4: Is cryptocurrency a physical coin? (1) Yes and (2) No

Response: Respondents have said that it is a physical coin, showing that they are not aware of the characteristics of cryptocurrency. 98 percent of the sample population have some basic idea about the digital currency, which is a sign in its favor.

Question 5: What are the cryptocurrencies you are aware of? (Mark all that apply) (1) Bitcoin, (2) Etherium, (3) Litecoin, (4) Dash, (5) Ripple, (6) Others, and (7) None of these

Response: 96 percent said that they are aware of cryptocurrencies in question 1. Of them, 91 percent have said that they are aware of Bitcoin. This is a multi-select question to find how any currencies people are aware of. Ethereum and Litecoin are the next popular currencies, followed by Dash. This response shows that people have made an effort in getting to know the available cryptocurrencies in the market.

Question 6: Do you know about the applications where cryptocurrencies can be used as payment? (Mark all that apply) (1) Online shopping, (2) Bill payments, (3) Travel transactions, (4) Digital asset transfers like properties and cars, (5) Advertising and media, (6) Private transactions without having the need to inform banks, (7) Hospitals and healthcare, and (8) Not aware

Response: This question is important as it tests the awareness of people about using cryptocurrencies practically. The survey is interested in knowing if the knowledge of people is just basic or they have ideas of the applications of the digital currency. If they are aware, they will move on to the next step of using it in real-time early in the near future. 76 percent of people are aware of its use in online shopping and 71 percent about its use in bill payments. The other applications are known by 30 to 40 percent of the people, which is a good sign to show their awareness. Though they may be motivated to apply in real-life applications, still it is a long step towards that goal.

Question 7: What makes you take an interest in cryptocurrency? (Mark all that apply) (1) Want to know what it is, (2) Currency of future, (3) Would like to use it as a payment source, (4) Would like to use it as an investment, and (5) Not interested

Response: This question wants to know the real interest of people towards cryptocurrencies, as this leads to other areas like payment and investment option. 88 percent have said they want to know what it actually is. Though 36 percent have said they have actually used in question 2 and 52 percent have expressed their willingness to use it in question 2, the real reason to pursue it lies behind the interest in knowing it. 76 percent of people are aware of its application in online shopping, but only 46 percent say here that they will use it as a payment source. So there are some inhibitions for them to use it, which is found out in the questions that will follow. Only 24 percent have said that they will use it as an investment. Though cryptocurrencies have been touted as the currency of the future, only 56 percent think so.

Question 8: What do you think are the advantages of cryptocurrencies? (Mark all that apply) (1) Low-cost transaction, (2) Immediate transfer, (3) Data protection, (4) Anonymity, (5) Going green because of paperless money, (6) None of these, and (7) No idea

Response: The number of responses got towards the advantages of cryptocurrencies is quite surprising. People who have used it only have said that it is of a low-cost transaction and gets transferred immediately. The other responses are only about 30 percent. 30 percent have agreed that they have no idea at all about the advantages. The responses cannot be straight forward compared

with other questions as they are of a multi-select type and the same person can have selected more than one option. Hence, no single pattern can be got from the number of responses.

Question 9: Why are you hesitant to use cryptocurrency? (Mark all that apply) (1) Poor security, (2) Price volatility (unstable and depends on demand), (3) Cannot be used in retail stores, (4) Not easy to cash out cryptocurrencies to fiat money, (5) Cannot be trusted as a savings, (6) No regulation, and (7) Can be used in wrong ways like money laundering, tax evasion, and terrorism

Response: 76 percent of people site poor security as the reason for not willing to use cryptocurrency-based payments. The other major reasons are that their application is limited and cannot be used as a payment medium in the frequently visited retail stores, price volatility of cryptocurrencies, difficulty in cashing out cryptocurrencies to fiat money, and fear of being used in wrong ways. All these concerns are prevalent from previous experiences. Safety measures have to be improved as is discussed in security resolutions discussed in chapter 5.3. The currency has to be stabilized to reduce volatility. The profound way to avoid abuses of technology is to instigate strong universal regulations and this lack of regulation is a concern expressed by 32 percent of the people for their hesitation in using cryptocurrencies. Steps to reduce these issues will go a long way in encouraging the common public to use cryptocurrencies for online trading.

Question 10: What do you feel are the security risks in cryptocurrencies? (Mark all that apply) (1) No data protection, (2) Not legal tender, (3) Can be traced back and hence no privacy to the user, (4) Hackers or viruses can wipe out Blockchain network, and (5) No idea

Response: This question is to find what the common people perceive as security risks in using cryptocurrencies. Despite the claim of cryptocurrencies that they are secure and tamper-proof due to their decentralized nature, there have been many instances of security attacks, leading to questions among the users. It is no wonder that people attributed security concern as the main reason for their hesitation in using cryptocurrencies. 72 percent of the people say that there is no data protection and 56 percent say that there is no privacy to the user as all transactions are made public. The transparency is a feature boasted by the cryptocurrency as a key feature in its security provision and this cannot be compromised because the users want privacy. This requires education on the users' part. 45 percent feel that it is not legal render due to not having strict regulations and 40 percent say there is a threat of hackers, which is a genuine reason. 34 percent say that they have no idea as they could not understand the working and the characteristics of cryptocurrencies. The security concerns expressed will be discussed with real-life examples in section 5.2 and the security resolutions in section 5.3.

Question 11: Do you think cryptocurrencies have a long-term future? (1) Yes, (2) No, and (3) Not sure

Response: Opinion is divided on whether cryptocurrencies have long term future. Ironically, only about 1/3rd of the sample say that it has a long-term future, even though 58 percent are willing to use crypto, 56 percent say it is the currency of future, and 43 percent would like to use it as a payment

source. About 1/3rd say that it does not have a long-term future and another 1/3rd say that they are not sure. Hence, through user response, it cannot be deduced how cryptocurrencies will fare in the future.

Question 12: Will you invest in ICO from a company (Fundraising where the public can buy crypto coins similar to shares)? (1) Yes, (2) No, and (3) Cannot say now

Response: ICO (Initial Coin Offering) are sold to investors as tokens to acquire legal tender or other cryptocurrencies (Kjarpal, 2018). This is considered as an investment like shares. In question 9 on hesitation in adopting cryptocurrencies, 26 percent of respondents have said that it cannot be trusted as savings. In question 10 on security risks, 45 percent have opined that there is no legal tender for cryptocurrencies. And 2/3rd of respondents have said that they do not believe that cryptocurrencies have a long-term future. At this backdrop, it is only logical that the respondents would not be willing to invest in ICOs as they do not trust it and has no legal tender. In this question, only 15 percent are willing to invest in ICO, whereas the other 85 percent are either undecided or are not willing to invest in ICO.

Question 13: Do you consider cryptocurrencies as an investment option? (1) Yes, (2) No, and (3) Not sure

Response: This is a direct question on whether the respondents will invest in cryptocurrencies, rather than ICO tokens. Again, only 20 percent have said that they will make an invest whereas the other 80 percent are either undecided or not willing. People willing to ICO were 15 percent whereas that in cryptocurrencies were 20 percent. There is not much difference. Hence, it can be summed up that people do not consider investment in cryptocurrencies as a viable option.

Question 14: Why do you not see cryptocurrency as an investment option? (Mark all that apply) (1) I do not believe in cryptocurrency as future, (2) Not sure of profit and returns, (3) Subject to scams and frauds, (4) Illegitimate, and (5) Not aware of this option

Response: These questions ask for reasons from people as to why they do not see cryptocurrencies as an investment option. 40 people say that they do not believe in cryptocurrency as future and 52 see it as illegitimate. Though this may contradict people's opinion on their willingness to use cryptocurrencies, it can be inferred that security risks play a major role in people's decision making. 49 people are not even aware that it can be used as an investment. Awareness of cryptocurrencies, its characteristics, and its applications will play a major role in influencing people's decision on considering it as an investment.

Question 15: Cryptocurrencies are more or less compared with gold rather than with money or stock exchange. If it is in par with gold, will you invest in it? (1) Yes, (2) No, (3) Maybe, and (4) Cannot say now

Response: Gold has always been considered as a safe and reliable investment due to its characteristics of price appreciation, stabilization, and legal tender. Cryptocurrency developers are proposing this digital currency in par with gold. The questionnaire wanted to know if cryptocurrency can be considered on par with gold, will people make an investment into it. The responses show that

willingness to invest has improved slightly but not considerably. 20 people say that they cannot say now and would like to see its performance in the future. Hence, it can be safely concluded that efforts from cryptocurrency manufacturers and standard regulations will help to bring people's trust over them and will help in its investment and adoption.

C. Analysis of Results

The key concern in online payment is a security issue, with Blockchain method being no exception to it. The security issues in Blockchain payment methods and earlier solutions for those security issues were studied in the literature review section. Recent solutions on security issues for Blockchain-based payments are discussed. This research work presents findings using literature on:

- Security issues arising out of Blockchain attacks - finding ways of attack and classifying the attacks
- Find out if any Blockchain attacks have been successful and if so, how did they succeed
- Resolutions to overcome security problems while using Blockchain as an online payment source in e-commerce applications
- Classification of abuses on Blockchain technology
- Preventing abuses of Blockchain technology

(i) Types and Classification of Blockchain Attacks

The types and classification of Blockchain attacks were studied in the literature review chapter. The major types of attacks identified were attacks on cryptocurrency wallet, time jacking attacks, 51% attack, double-spending attacks, selfish mining, and fork problems. Some of these attacks were said to be hypothetical in the early phases of cryptocurrency foundation but were later found to have occurred in reality. Attacks like time jacking led to other types of attacks like double-spending. The occurrence of these attacks in real-time is discussed in the next subsection.

The attacks on cryptocurrencies can be classified into different categories:

- Attacks to slowdown cryptocurrency adoption
- Attacks to reduce the efficiency of cryptocurrency infrastructure
- Attacks to slow down the development of cryptocurrencies

Some attacks have a high probability of getting executed while some do not. The damage could be less or very high (CryptoBullsAdm 2018). At this outset, the Blockchain attacks that were successful are studied in the next section.

(ii) Are any Blockchain Attacks Successful and How did they Succeed?

The characteristics of Blockchain technology like distributed and decentralized consensus, trust-free transactions without any intermediaries, immutability distributed ledger, embedded cryptographic mechanisms, and anonymity were supposed to make it a breakthrough technology for registering, recording, verifying, and managing transactions and hence capable of preventing frauds and attacks (Xu 2016). However, hackers were able to find loopholes in the technology and used it to carry out

various types of attacks. The attacks were considered to be hypothetical but many of them were executed practically. This section discusses the types of attacks that were carried out successfully and the way in which they succeeded.

a. Attack on wallet software

Cryptocurrencies are difficult systems to hack and hence customers are targeted. Customers are supposed to be more responsible in a decentralized financial services system. Client software exploits like theft of wallet are one of the client-side attacks employed. The first wallet attack on Bitcoin cryptocurrency was reported in June 2011 By Symantec at the Bitcoin Bubble, which was done by a malware Infostealer.coinbit. When this Trojan is run, it searches for bitcoin wallets in Windows machines and emails the information to the attacker through a serer in Poland. Another similar, but much more complicated Trojan DevilRobber targets Mac machines where it destroys wallet files, collects system information, and collects username and passwords. In this case, even encrypted wallets could not prevent the malware from stealing their wallet contents. A solution to overcome this issue is encrypting wallet private keys with the Advanced Encryption Standard symmetric key algorithm (Latifa et al. 2017).

b. Time jacking

Time jacking is executed by altering the timestamp of a network node and deceiving it to forming an alternate blockchain. Consequences of this process are an increase in the chances of double spending and wastage of computational resources. This attack is a theoretical vulnerability and no cases of time jacking attack have been reported so far ("Hypothetical Attacks on Cryptocurrencies" 2018). However, 3 cases of 51% attack in April and May 2018 reported by privacy-centric digital currency Verge (VxG), showed that the attack was executed by altering the timestamp of the target node. A malicious miner was able to mine blocks with spoofed timestamp deceiving the network to think that the new block was mined an hour ago and added it to the Blockchain. The next mined block was also added immediately to the network. The attacker was able to mine one block per second in this manner and accumulated 250,000 VxG in the first attack on April 4, 2018 (Lielacher 2018).

c. 51% attack

51% of attacks or majority attacks occur when miner(s) control more than 50 % of the network's hashing power so that they can create a fork of the network and make a double-spend attack. The attacking miners can reverse and erase transaction history and can prevent new blocks from confirming. Since 51% attack requires a lot of computing power to execute, they are mostly restricted to smaller coins and Blockchain networks. 51% is not due to security flaws or vulnerabilities but is a result of the manipulation of technology.

An example of this majority attack is the attack on Krypton network using a dual-prolonged approach that combined majority hashing power with a distributed denial-of-service (DDoS) to artificially increase the relative hashing power of the attacking party. During this attack, about 21,000 KR was stolen from Krypton network, which was sent to Bittrex and exchanged for Bitcoin. The

attackers then reversed the transaction by rolling back the Blockchain and took away the bitcoins. Since a majority attack on the bitcoin network will require large computing power, it was theoretically assumed that such an attack will not take place. But it was proved wrong when in July 2014, Ghash.io, one of the popular bitcoin mining pools, exceeded the 51% hashing power of the total bitcoin network. Though they did not make any attack, they showed that majority attacks are possible in a network as big as bitcoin and Ethereum (Spirkovski 2018).

d. Double spending

Double spending attack is one where the attacker makes more than one transaction with the same coin. An example of a double-spending attack on Bitcoin Gold (BTG) shows the involvement of a 51% attack, resulting in double-spending. BTG lost $17.5 million in this attack on 16 May 2018 (Osborne 2018). BTG found out that double-spending attacks were launched against BTG exchanges, rather than individuals. The team reported that an unknown party who had access to large amounts of hash power used 51% attack to carry out "double spending" attacks. 51% attacks force reorganizations in the Blockchain. In double-spending, confirmed transactions are reversed and the money is spent again. Double spending also prevents miners from mining valid blocks (Osborne 2018).

e. Selfish mining

Selfish mining is one of the major attacks in Blockchain networks. Selfish mining is one where a miner successfully mines a block but does not broadcast it to other miners. The miner can keep on adding blocks to his secret block, creating a chain. In a Blockchain network, the longest chain is considered as the correct one. Hence the blocks of other miners with small chains are invalidated and become orphaned. A selfish miner makes transactions with the hidden chain before they are invalidated. In essence, they have never paid for their purchases. Monacoin Blockchain was attacked in Japan by trying to send it to exchanges outside Japan to exchange it with other coins before the hidden chains are revealed in the Blockchain. The malicious miner had about 57 % hash rate or computing power to execute selfish mining. The attack was identified on May 18th, 2018 but the crypto coin authorities stating that the miner has been trying to exploit for about 6 months (Gutteridge 2018).

f. Fork problems

A fork is a divergence in a Blockchain when part of a network has different views on transaction history than another part of the network. The fork can occur naturally or can be purposefully introduced. Forks can be introduced by miners or cryptocurrency users. Blockchains were very long and were managed by a few people. They were split or forked so that many people can work on small chains. Large cryptocurrencies split or fork their currencies to generate new ones. For instance, bitcoin underwent a fork on October 24, 2017, to create a new coin namely bitcoin gold cryptocurrency. This was created with the aim of allowing more people to mine bitcoin gold with less

powerful machines. Expert opinion is divided on whether a fork is good or bad for a Blockchain (Kharpal 2017).

(iii) Resolutions to Overcome Security Problems with Blockchain Online Payment

Some of the major security problems in Blockchain networks were discussed in the literature review. Their occurrence in the real world was substantiated with evidence in the previous section. Some latest resolutions to overcome security issues are discussed in this section. Irrespective of the type of attack, general resolutions like detection technologies, identity for Blockchains, regulations, and wide adoption of the technology are some ways of securing Blockchains. Also, the recent resolutions for some types of attacks have been discussed.

a. General Resolutions

Detection technologies: Techniques like machine learning and data-mining algorithms can be used in applications that detecting fraud and intrusions in Blockchain trading. Supervised machine learning approaches like deep-learning neural networks, support vector machines (SVM), and Bayesian network can help to find outlier behavior (Xu 2016).

Identity Blockchain: Identity is protected by private keys in a Blockchain, thereby making it vulnerable to digital identity theft. Loss of key leads to loss of identity in the network. Identity and reputation system in a Blockchain network can be built using measures like fingerprint records and tracking life events like birth, schooling, purchasing homes, buying cars, and opening bank accounts.

Regulation: Administrative functions by the government are eliminated in Blockchain due to its decentralized consensus and anonymous characteristics. However, these characteristics can give rise to maliciousness and illegality. Government bodies and lawmakers across the world should cooperatively develop and implement laws, policies, and regulations to govern Blockchain applications.

Wide adoption: Mechanisms and protection technologies associated with Blockchain technology can work effectively only when the technology is widely adopted by the majority of the society (Xu 2016).

Various malicious attacks in Blockchain and the potential strategies to encounter them are shown in Table 3.

Table 3: Malicious Attacks on Blockchain and their Defensive Measures (Xu 2016).

Malicious Attack	Definition	Defensive & Preventive Measures
Double Spending	An individual makes more than one payment using one body of funds.	The complexity of the mining process
Record Hacking	Records in the ledger are modified or fraudulent transactions are inserted into the ledger.	Distributed consensus

51% Attack	A single miner node with more computational resources (51%) than the rest of the network nodes dominates the verification and approval of transactions.	Detection techniques; wide adoption of the Blockchain technology
Identity Theft	The private key of an individual is stolen.	Identify relevant Blockchain
Illegal Activities	Parties transact illegal goods or commit money laundering.	Detection techniques; laws and regulations
System Hacking	The programming codes and systems that implement blockchain are compromised.	Robust systems and advanced intrusion detection methods

b. Attack on wallet software

Some measures of securing cryptocurrency wallet are ((Rajput 2018) & (Latifa et al. 2017)):

- Encryption of private keys of wallet with Advanced Encryption Standard Symmetric-key algorithm
- Combination of private keys and multi-signature security. Multi-level authentication is operated by users.
- Hardware wallet storage – Securing through cold storage by storing the coin values in a hardware wallet. This method does not require an internet connection and is called an offline method.
- Backing up entire wallet, encrypt backups, using multiple locations to backup wallet data, and regular backup

c. Time jacking

Attacks like time jacking have had near-zero occurrences and hence no new techniques have been developed to overcome that attack. Since it is always associated with double-spending, most of the security measures for double-spending also hold goods for time jacking attacks.

d. 51% attack

Many techniques are in use and many more are being explored to counter 51% attack. One such technique is delayed Proof of Work (dPoW) mechanism which stores backups of the Blockchain onto the cryptocurrency ledger. This mechanism takes a snapshot of every Blockchain to record the balance of each and every address. This snapshot is written into the security services' main chain whose snapshot is also taken. All this information is saved in a block in the Blockchain. This process occurs every 10 minutes. An attacker has to alter the currency as well as security services' network before altering or destroying the backups of Blockchain within a window of 10 minutes. There is not enough time to launch a successful 51% attack. This dPoW mechanism acts as two-factor authentication (Daniel 2018).

e. Double spending

The time between transaction broadcasting and its publication in a block is called as zero-confirmation transactions. P´erez-Sol`a et al. (2017) propose a model to overcome double-spending attacks occurring on zero-confirmation transactions. Through this model, the attacker will be punished

to attempt double-spending as he will face the risk of losing a large number of bitcoins greater than the amount of double-spending. This solution especially benefits fast-payment scenarios.

f. Selfish mining

Selfish mining is the major type of attack and hence many solutions are being explored and put in place to prevent and overcome this type of attack. Heilman (2014) proposed a defense mechanism against selfish mining by raising the minimum power required to selfishly mine profitably from 25% to 32%. This solution uses unforgeable timestamps to make sure that a particular block was generated not beyond the timestamp. This model offers incentives to miners of selfish mining cartel to leak information on compromised infrastructure. Hence the selfish miners will evade from cooperating for selfish mining. Another way of overcoming selfish mining is to increase the threshold level at which selfish mining is effective (Eyal & Sirer 2013). The current threshold is close to zero. The authors proposed a backward-compatible modification that raises the threshold of the cryptocurrency to 1/4.

g. Fork problems

Forks can be regarded as a necessary evil as the advantages they bring in are more compared to the negative changes. According to Adams (2018), forks can be considered as equal to a software or protocol updates to Blockchain network. Forks are formed as a result of technical disagreements, to reverse transactions in Blockchain, and to add new features or functionality to the network. Forks bring in negative consequences like infighting and collision between miners and developers of a cryptocurrency. Hence a thorough understanding of the forking process and the reason for forking is needed to judge if its impact is positive or negative on a cryptocurrency at a given point of time.

(iv) Preventing Abuses on Blockchain Technology

The literature review showed that Blockchain technology undergoes abuses like links to child abuse contents, tax evasion, money laundering, links to drugs, financing illegal activities, and terrorism. The ways of preventing these abuses are being explored. One of the major factors that contribute to these types of abuses is lack of international regulation of cryptocurrencies and Blockchain networks.

Different countries look upon cryptocurrencies in a different manner for taxation purpose. For instance, Israel taxes cryptocurrency as an asset, Switzerland as foreign currency, Argentina as subject to Income Tax, and Bulgaria as a financial asset, and so on. This is only one example to show the different perspectives of different countries on cryptocurrencies, making it difficult to regulate under one roof and policy (Global Legal Research Directorate Staff 2018).

To avoid abuses by participants of cryptocurrency, the concerned states must issue regulations on the subject to avoid the negative effects on the economy and international institutions. In the absence of state regulation, the cryptocurrency market has to implement self-regulation on the use of cryptocurrencies to avoid abuses and attacks (“Cryptocurrencies: International Regulation and Uniformization of Practices” 2017).

5. Conclusions and Future Work

Cryptocurrencies have evolved as an online payment medium over the course of years since their inception as digital currencies. This research paper studied one area of its application, namely e-commerce payment. Similar to traditional online payment, payment with cryptocurrencies also has issues, main among them being security concerns. The major security concerns were identified and discussed in the literature review. Resolutions to overcome security concerns were studied using literature and presented as results of the study.

The research employed a questionnaire on cryptocurrencies to know the extent people are willing to use it and the reasons for their unwillingness. The results showed that security concerns and digital currencies not being legal tender are the main reasons for people's hesitation in adopting cryptocurrencies for applications. The resolution for abuses of Blockchain technology is to have a centralized global regulatory body. Presence of universal governance will subside fears of cryptocurrencies not being legal tender. The fear of illegitimacy holds back people's investments in cryptocurrencies and a central governance system will help in overcoming people's fears and attract investments.

The responses showed security issues as the main reason for users' unwillingness in adopting cryptocurrencies as a payment medium. Resolutions are continuously being developed and employing appropriate ones will help to tide over this problem. Another point of study here is to know if cryptocurrencies have a future and this was judged by people's views on it being an investment option. This idea of investment did not sit well with the respondents. They quoted security concerns and cryptocurrency is not legal tender as the main reasons for not investing in the digital currency. Security resolutions were discussed earlier in this chapter. Proper regulations and global policies will make cryptocurrencies a reliable and stable currency so that people will not hesitate to use it. This idea has also been discussed in resolutions to overcome abuses of Blockchain.

This research work has studied the security attacks and abuses on cryptocurrencies. The major security issues were discussed and resolutions were found only for those issues. Besides these attacks, there are many other security issues. All these attacks and abuses could be studied as a separate research subject. Similarly, an extensive study of cryptocurrency resolution is another area of research.

References

"*4.1 Electronic Payment Systems (EPS)*". n.d. Available from: http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf.

Abner, B. 2015. *The pros and cons of using bitcoin for payments*. The Business Journals. Available from: https://www.bizjournals.com/bizjournals/how-to/technology/2015/08/the-pros-and-cons-of-

using-bitcoin-for-payments.html [09 Jul 2018].
Acosta KK 2008, *Online Payment Process, E-Business technologies*, Available from: https://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-Online-Payment-Process-Kathleen.pdf.
Adams, C. 2018. *Everything You Need to Know About Cryptocurrency Forks*. Available from: https://www.investinBlockchain.com/cryptocurrency-forks.
Barber, S., Boyen, X., Shi, E., & Uzun, E. 2012. Bitter to better-how to make bitcoin a better currency. *Lecture Notes in Computer Science*, 7397, 399-414, Springer-Verlag. Available from: https://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf.
Bauerle, N. 2018. *How Does Blockchain Technology Work?* Available from: https://www.coindesk.com/information/how-does-Blockchain-technology-work/ [09 Jul 2018].
Boverman, A. 2011. *Timejacking & Bitcoin*. Culubas. Available from: http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html.
Charlesworth, A. n.d. *Doing research: Planning, Risk & Reflection*. Available from: https://www.cs.bris.ac.uk/Teaching/learning/how-to-lectures/planning-risk-reflection.pdf.
Claburn, T. 2018. *Bitcoin's Blockchain: Potentially a hazardous waste dump of child abuse, malware, etc.* Available from: https://www.theregister.co.uk/2018/03/19/ability_to_dump_illegal_content_in_bitcoins_Blockchain_puts_participants_in_peril/ [10 Jul 2018].
"*Cloud Customer Architecture for Blockchain*" 2017. Cloud Standards Customer Council. Available from: http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-Blockchain.pdf.
"*Cryptocurrencies: International Regulation and Uniformization of Practices*". 2017. Available from: https://www.uncitral.org/pdf/english/congress/Papers_for_Congress/29-DOLES_SILVA-Cryptocurrencies_and_International_Regulation.pdf.
CryptoBullsAdm. 2018. *Classification of Attacks on Bitcoin***.** Available from: https://cryptobulls.info/classification-attacks-bitcoin [10 Jul 2018].
"*Cryptocurrency Wallet Guide: A Step-By-Step Tutorial*". 2018. Available from: https://blockgeeks.com/guides/cryptocurrency-wallet-guide [09 Jul 2018].
Daisyme, P. 2018. *Issues with Blockchain Security*. Available from: https://www.business2community.com/tech-gadgets/issues-Blockchain-security-02003488.
Daniel. 2018. The Anatomy of a 51% Attack and How Komodo can help Prevent One. Available from: https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one.
"*Data Collection*" 2017. research-methodology.net, Available from: https://research-methodology.net/research-methods/data-collection/ [22 Jul. 2018].
'*Distributed ledger technology in payment, clearing, and settlement*" 2017. Bank for International Settlements 2017. Available from: https://www.bis.org/cpmi/publ/d157.pdf.
Dumitrescu, G.C. 2017. *Bitcoin – A Brief Analysis of the Advantages and Disadvantages*. Available

from: http://www.globeco.ro/wp-content/uploads/vol/split/vol_5_no_2/geo_2017_vol5_no2_art_008.pdf.
"*E-Commerce: Purchasing and Selling Online*" 2013. Part of Ontario's e-Business Toolkit, Available from: https://dr6j45jk9xcmk.cloudfront.net/documents/435/medi-booklet-e-commerce-accessible-e-final.pdf.
Eyal, I., & Sirer, E.G. 2013. *Majority is not Enough: Bitcoin Mining is Vulnerable*. Available from: https://arxiv.org/pdf/1311.0243.pdf.
Foley, S., Karlsen, J.R., & Putniņš, T.J., 2018. *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* Available from: https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through [10 Jul 2018].
Global Legal Research Directorate Staff. 2018. *Regulation of Cryptocurrency Around the World*. Available from: http://www.loc.gov/law/help/cryptocurrency/world-survey.php#eu.
Gutteridge, D. 2018. *Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack*. Available from: https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack.
Haughey, D 2014, *Smart Goals*. Available from: https://www.projectsmart.co.uk/smart-goals.php. [25 May 2018]
Heilman, E. 2014. *One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner*. Available from: https://eprint.iacr.org/2014/007.pdf.
"*How Blockchain architecture works? Basic Understanding of Blockchain and its Architecture*.**"** 2018. Zignuts Technolab. Available from: https://www.zignuts.com/blogs/how-Blockchain-architecture-works-basic-understanding-of-Blockchain-and-its-architecture/ [09 Jul 2018].
"*How the Blockchain Works*". 2018. RubyGarage. Available from: https://rubygarage.org/blog/how-Blockchain-works [09 Jul 2018].
"*How to Send and Receive Cryptocurrency*". 2018. Cryptocurrency Facts. Available from: https://cryptocurrencyfacts.com/how-to-send-and-receive-cryptocurrency [09 Jul 2018].
"Hypothetical *Attacks on Cryptocurrencies*". 2018. Blockgeeks. Available from: https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies.
Jaag, C. & Bach, C. 2016. *Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services*. Swiss Economics Working Paper 0056. Available from: http://cryptecon.org/wp-content/uploads/2016/08/0056JaagBach.pdf.
Johnson, R. 2017, *5 Major Types of Ecommerce*, Available from: https://bizfluent.com/info-8788484-5-major-types-ecommerce.html. [25 May 2018]
"Know *more about Blockchain: Overview, Technology, Application Areas and Use Cases*" 2018. MEDICI, Available from: https://gomedici.com/an-overview-of-Blockchain-technology.
Karame, G.O., Androulaki, E. & Capkun S. 2012. Double-Spending Fast Payments in Bitcoin. In *CCS'12 Proceedings of the 2012 ACM conference on Computer and communications security*, October 16–18, 2012, Raleigh, North Carolina, USA., 906 – 917. Available from:

https://www.eecis.udel.edu/~ruizhang/CISC859/S17/Paper/p9.pdf.
Kharpal, A. 2017. *Bitcoin splits again, creating a new cryptocurrency called bitcoin gold that then plunged 66%*. CNBC. Available from: https://www.cnbc.com/2017/10/25/bitcoin-gold-price-plunges-what-is-hard-fork.html.
Kharpal, A. 2018. *Tokenization: The world of ICOs. CNBC.* Available from: https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html.
Kulkarni, A 2017. *Blockchain; Applications in payments*. Available from: https://www.europeanpaymentscouncil.eu/news-insights/insight/Blockchain-applications-payments.
Latifa, E., Ahemed, E.K.M., Mohamed, E.G., & Omar, A. 2017. Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures. *Journal of Internet Banking and Commerce, December 2017,* 22(3). Available from: http://www.icommercecentral.com/open-access/Blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.pdf.
Lielacher, A. 2018. *More 51% Blockchain attacks expected.* Available from: https://bravenewcoin.com/news/more-51-Blockchain-attacks-expected.
Lin, I. & Liao, T. 2017. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5), 653-659. Available from: https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf.
Martucci, B 2018, *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives*, SparkCharge media, LLC, Available from: https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/ [25 May 2018].
"Methods *of data collection – Primary and Secondary data*" 2016, BBA|mantra, Available from: http://www.bbamantra.com/methods-of-data-collection-primary-and-secondary-data/ [22 Jul. 2018].
Mosakheil, J.H., 2018. Security Threats Classification in Blockchains. Thesis submitted to: *St. Cloud State University - the Repository at St. Cloud State*. Available from: http://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1093&context=msia_etds.
Niranjanamurthy, M & Chahar, D 2013, The study of E-Commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(7). Available from http://www.ijarcce.com/Upload/2013/july/69-o-Niranjanamurthy%20The%20study%20of%20ECommerce%20Security%20Issues%20and%20Solutions.pdf.
Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. 2017. Blockchain. *Bus Inf Syst Eng*, 59(3), 183–187. Available from: http://www.cs.unibo.it/~montesi/CBD/Articoli/2017Blockchain.pdf.
Osborne, C. 2018. *Bitcoin Gold suffers double spend attacks, $17.5 million lost***.** ZDNet. Available from: https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost.
Pauw, C. 2017. *Multi Cryptocurrency Payment Gateway, Explained*. Cointelegraph. Available from: https://cointelegraph.com/explained/multi-cryptocurrency-payment-gateway-explained.
"*Payment Processing – A Timeline of Steps Involved in Online Payment Processing*" 2018. Allied

Wallet, Ltd. Available from: https://www.alliedwallet.com/blog/blog-posts/payment-processing-timeline-steps-involved-online-payment-processing/ [06 July 2018].
Perez-Sol ´ a, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera- ` Joancomart´I, J. 2017. Double-spending prevention for bitcoin zero-confirmation transactions. Available from: http://eprint.iacr.org/2017/394.
Peters, G.W. & Panayi, E. 2015. *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*. Available from: https://arxiv.org/pdf/1511.05740.pdf.
Rajput, M. 2018. Valuable Steps to Make Your Bitcoin Wallet Safe and Secure. Available from: https://www.globalsign.com/en/blog/steps-to-make-your-bitcoin-wallet-safe-and-secure.
"*Research Design*" 2017. research-methodology.net, Available from: https://research-methodology.net/research-methodology/research-design/ [22 Jul. 2018].
Ruppert, P. 2017. Privacy, Tax Evasion, and the Development of Cryptocurrencies. *Georgetown Law Technology Review*. 398. 1(2). Available from: https://www.georgetownlawtechreview.org/privacy-tax-evasion-and-the-development-of-cryptocurrencies/GLTR-04-2017.
Schadeck, W.X. 2017, *What is Blockchain, really? (An intro for regular people)*, Medium, Available from: https://medium.com/@wen_xs/what-is-Blockchain-really-an-intro-for-regular-people-e51578d98a96.
Sharma, T.K., 2018. *How does Bitcoin Money Laundering work?* Blockchain Council. Available from: https://www.Blockchain-council.org/Blockchain/how-bitcoin-money-laundering-works. [10 July 2018].
Spirkovski, Z. *Strength in Numbers: A Brief History of 51% Attacks*. Crypto-News.net. Available from: https://www.crypto-news.net/strength-in-numbers-a-brief-history-of-51-attacks.
"*Types of Variables – Categorical*" 2017, University of Minnesota, Available from: https://cyfar.org/types-variables-categorical.
"*Types of Variables – Continuous*" 2017, University of Minnesota, Available from: https://cyfar.org/types-variables-continued-0.
Thein, A.Z.P. 2017. *Cryptoterrorism: Do Cryptocurrencies Facilitate Terrorism?* marketMogul. Available from: https://themarketmogul.com/cryptoterrorism-far-cryptocurrencies-come-financing-terror/ [Last accessed: 10 July 2018].
Vivo, M.D. 2018. *Why and How to Accept Cryptocurrency on Your Website*. Singe Grain. Available from: https://www.singlegrain.com/Blockchain/why-and-how-to-accept-cryptocurrency-on-your-website/ [Last accessed: 09 July 2018].
Vyas, A.A. & Lunagaria, M. 2014, Security Concerns and Issues for Bitcoin, *International Journal of Computer Applications (IJCA)*, 10-12, Available from: https://pdfs.semanticscholar.org/4751/e99514948c2cbef0f6e4a12e65c72f75ae8.pdf.
"*What is cryptocurrency — and how can I use it*?" 2018. FinderUS. Available from:

https://www.finder.com/what-is-cryptocurrency.
Xu, J.J. 2016. Are Blockchains immune to all malicious attacks? Xu Financial Innovation, 2(25). Available from https://pdfs.semanticscholar.org/780c/d51bdf55183f3d440d8e7d84b17526c08d5e.pdf.