Enhancing Trust in the Cryptocurrency Marketplace: A Reputation Scoring Approach

Sudip Bhattacharyya[1], Dan Freeman[1], Timothy McWilliams[1],
Craig Hall[2], Pablo Peillard[2]

[1]Southern Methodist University
6425 Boaz Lane
Dallas, TX 75205
{sbhattacharyya, freemand, tmcwilliams}@smu.edu

[2]Caudicum
1920 McKinney Ave., Suite 750
Dallas, TX 75201
craig@caudicum.com, pablo12335@gmail.com

Abstract. Trust is paramount for the effective operation of any monetary system. While the distributed architecture of blockchain technology on which cryptocurrencies operate has many benefits, the anonymity of users on the blockchain has provided criminal users an opportunity to hide both their identities and illicit activities. In this paper, we present a scoring mechanism for cryptocurrency users where the scores represent users' trustworthiness as safe or risky transactors in the cryptocurrency community. In order to distinguish law-abiding users from potential threats in the Bitcoin marketplace, we analyze historical thefts to profile transactions, classify them into risky and non-risky categories using several machine learning techniques, and finally calculate a reputation score for every unique user based on their past association with any unlawful Bitcoin incident. The Support Vector Machine model based on two key attributes produces an accuracy of 86% and is considered the most applicable for our dataset. Our reputation score ranges from 0 to the total number of transactions by a given user where a higher score indicates greater trustworthiness in making Bitcoin transactions. This score helps to identify reputable users and, therefore, acts as a guideline for safe Bitcoin transactions. In the cryptocurrency marketplace, our self-attestation metric in the form of a reputation score offers a foundation for enhancing trust between transacting parties.

1 Introduction

Recent advances in distributed and parallel networking using Internet-ubiquitous accessible services are allowing a re-engineering of previously centralized system design and authority. New shared access has created the opportunity for non-mediated trust through the use of transparency and immutability within a public historical record.

This record is maintained by a community of users rather than a third-party mediator declaring what is the trusted record based on their assessment.

While this disintermediation of third-party authorities using blockchains and smart contracts is in its early development for many applications, digital assets like cryptocurrency have operated under a distributed model for almost a decade. The lack of regulation brings the challenge of avoiding fraud and market manipulation in this borderless technology. Such behavior and norm policing are traditionally handled with sanctions and settlements by designated central authorities such as governments and central banks.

The essential requirement for money to work is trust. Trust has worked as a pillar for monetary exchanges at every stage of civilization starting from a barter system to the broader aspects of a society-wide monetary system. Without trust, the honest exchange of goods or services for currency is infeasible and cryptocurrency is no exception in this regard. A trustworthy environment is essential for the widespread acceptance of cryptocurrency.

Transparency is a great creator of trust and it has a long history as a tool for oversight in anti-corruption, antitrust and anti-money laundering movements. Transparency in money and banking have frequently focused around a few sentences written by U.S. Supreme Court Justice Louis Brandeis. In 1914, two years before his time on the high court began, Brandeis wrote in his book *Other People's Money and How the Bankers Use It* "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman. And publicity has already played an important part in the struggle against the Money Trust" [1].

Transparency is not new, but when combined with distributed blockchain records, it becomes a powerful tool for enhancing trust and reputation among participants in a society. The parallels between Brandeis' world in 1914 and the world today are striking. His writings that followed laid out the details of suspect transactions and his proposal to require additional information. "[T]he disclosure must be real . . . To be effective, knowledge of the facts must be actually brought home to the investor" [1].

In spite of its secure environment, the cryptocurrency marketplace has experienced numerous unlawful activities since its inception in 2009. These incidents have caused its users to lose more than $2 billion in assets [2]. A trust mechanism in the form of a reputation score for all users operating in a blockchain network could possibly alleviate some of the unlawful activities that too often negatively impact lawful users. Our reputation scoring mechanism enables users to identify and avoid risky parties while making transactions.

In order to mitigate risk, in this paper, we propose a scoring mechanism that interprets the trustworthiness of a user on the cryptocurrency network. The proposed score is developed in three steps. The first step is the creation of a blacklist based on the historical thefts on Bitcoin exchanges. The blacklist provides law-abiding users with a list of potentially criminal entities with which they should avoid making transactions. The second step involves a classification task to differentiate the honest users from the malicious ones who purposefully enter the network to gain an undue financial advantage. Based on the classification, a metric in the form of a risk score is developed to indicate a user's degree of involvement in malicious transactions. The risk score metric serves as the basis for an improved metric in terms of a reputation score.

We train multiple machine learning algorithms to classify historical Bitcoin transactions for identification of any underlying pattern. Our support vector machine model produces a classification accuracy of 86% accuracy and an F1-score of 0.89 based on two attributes: the number of transactions in a block and the number of inputs in a transaction. This model has correctly classified all the risky transactions that occurred in reality.

With a successful classification algorithm, a scoring mechanism is designed to create a separator between different categories of users. Users with a reputation score below a certain threshold are identified as potential offenders. We propose to blacklist these users and restrict them from any further involvement in a cryptocurrency network. A continuously updated blacklist works as an operating manual for safe transactions on the Bitcoin network.

The remainder of this paper is structured as described here. Section 2 contains an overview of blockchain and the current cryptocurrency marketplace. In Section 3, we describe how to protect cryptocurrency from external attacks. Section 4 outlines the creation of the blacklist and our scoring approach in detail. We describe the dataset used in this study in Section 5. Section 6 contains the machine learning algorithms that we use and the corresponding measurements of the performance of the models. In Section 7, we present our results and analyses. We examine the ethical implications of profiling and scoring cryptocurrency users in Section 8. In Section 9, we present conclusions from our analyses. We highlight future work and potential extensions of our work in Section 10.

2 Blockchain and the Emergence of Cryptocurrency

Put simply, blockchain is a distributed ledger as shown in Figure 2.1, and cryptocurrencies are products that operate using a blockchain network. Cryptocurrency is a medium for exchanging assets between individuals. It is defined as a digital currency or asset for which transactions are made in an environment secured by a cryptographic encryption-decryption mechanism. The world's first cryptocurrency, known as Bitcoin, was conceptualized by Satoshi Nakamoto, a pseudonym of a person or a group of people, in 2008 [3]. The platform for cryptocurrency transactions is known as blockchain which was described by Satoshi as "a peer to peer electronic cash system" [4].

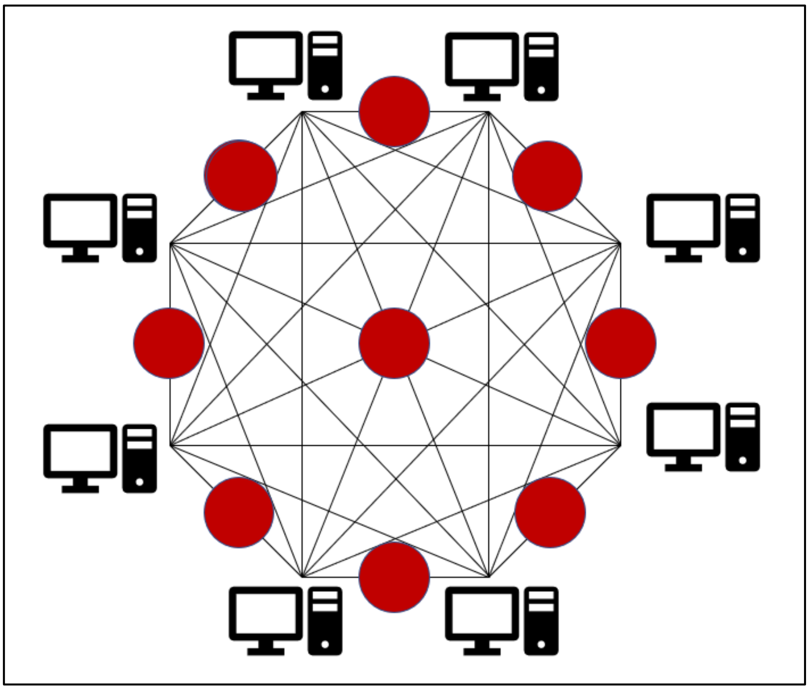


Figure 2.1. Standard blockchain network.

In blockchain, transactions are periodically recorded in a chain of blocks and stored across multiple computers or servers, known as nodes, distributed over the network. Unlike ledgers in our conventional banking system, blockchain has no single point of control. The nodes in blockchain cooperate to distribute the complete blockchain to each node and to verify that new blocks that a node attempts to add to the blockchain contains valid transactions. Blockchain is developed based on certain characteristics of a distributed ledger system: cryptography, replication of ledger and immutability.

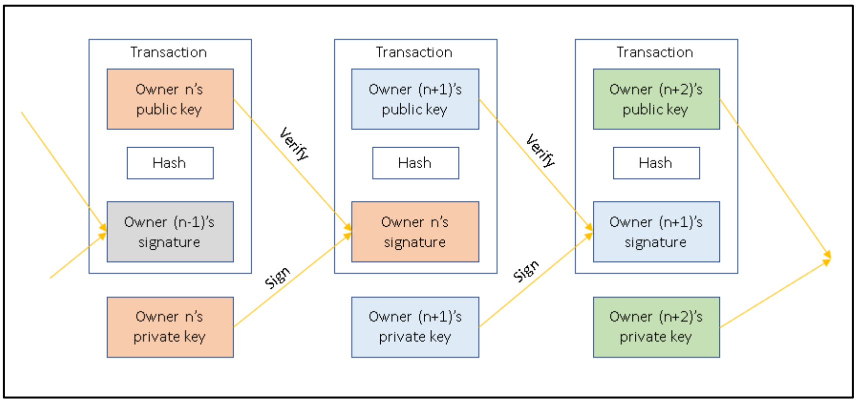


Figure 2.2. Blockchain security protocol.

Transactions on a blockchain are made secure with the use of public key ciphers and secure hash functions which is displayed in Figure 2.2. A public key infrastructure ensures authenticity and non-repudiation of a transaction. The secure hash functions ensure the integrity of the transactions and the blocks. When a sender approves a transaction along with its amount, a fee is paid to the miners who validate the transaction and add it to the ledger and the recipient's public key. The transaction is digitally signed using the sender's private key and then broadcast to the entire network on behalf of the sender. Network nodes then validate the authenticity of the transaction while verifying the sender's signature. Once verified by a majority of nodes, the sender's transaction is ready to be completed and added to a block. After verification, the recipient receives the asset from the transaction, where the asset is sent encrypted using the recipient's public key. After the transaction is complete, the transaction gets recorded along with other transactions in a block, or a new block is created in the distributed ledger system, and all the nodes receive a replication of the ledger updated with the new block appended. With the concept of this replicated ledger, blockchain maintains transparency, eliminates the chance of dispute and thereby makes the intermediaries unnecessary. Moreover, the identity of any user is masked with a hashed communication which ensures anonymity on a blockchain. A typical cryptocurrency transaction on a blockchain is illustrated in Figure 2.3.

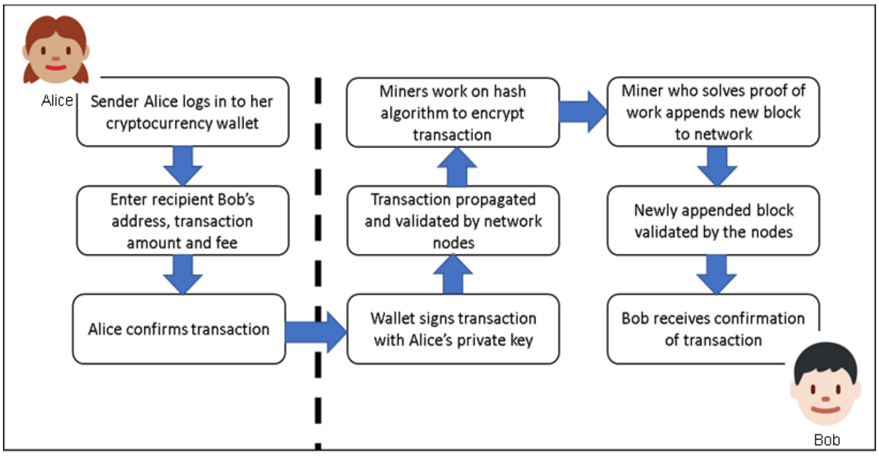

Alice
Sender Alice logs in to her cryptocurrency wallet
Enter recipient Bob's address, transaction amount and fee
Alice confirms transaction
Wallet signs transaction with Alice's private key
Transaction propagated and validated by network nodes
Miners work on hash algorithm to encrypt transaction
Miner who solves proof of work appends new block to network
Newly appended block validated by the nodes
Bob receives confirmation of transaction
Bob

Figure 2.3. Blockchain transaction cycle.

Another key feature of the blockchain is immutability. After a transaction is added to the network, it is impossible to erase it. Only a reverse transaction can be added to nullify the effect of the erroneous or unintentional transaction. This immutable nature of the blockchain makes the length of the chain ever-growing. The advantages of a blockchain are summarized in Table 2.1.

Table 2.1. Blockchain advantages.

Advantages	Description
Decentralization	In contrast to a centralized system, a blockchain is distributed and replicated across nodes connected in a distributed network. The network operates peer-to-peer, with the nodes together managing the blockchain.
Durability and robustness	Since it is built on the Internet, blockchain automatically inherits the durability of the Internet. Moreover, since it cannot be controlled by any single entity or node and there is no single point of failure, blockchain is expected to operate as a robust system.
Transparency and incorruptibility	Blockchain works using a consensus. A self-auditing system reconciles transactions in regular intervals. Any block of transactions is visible to all the participants, and data cannot be altered once validated and entered in the chain.
Security	With a distributed architecture, a threat of attack on any centralized point is eliminated. Moreover, the proof-of-work mechanism and the use of hash functions and public-private keys make the blockchain very secure from attacks.

As part of the Bitcoin concept, Nakamoto developed the first-ever blockchain database where the genesis block (the first block) has a timestamp of 18:15:05 GMT on 3 January 2009 [3]. Since the introduction of Bitcoin in 2009, the world economy has experienced an exponential growth both in terms of market capitalization as well as in the number of users in the cryptocurrency market. In the past few years, the cryptocurrency market has experienced an exponential growth in the number of active users, i.e., in the number of unique public keys in the network. The current number of users is reported to be more than 23 million and is expected to reach 200 million by 2024 at the present growth rate [5].

The cryptocurrency market is extremely volatile and sensitive to market demand. In a short span of 9 years, cryptocurrencies have become a multi-billion-dollar marketplace worldwide. Even though the market was conservative in nature for the first few years, it started to gain momentum in 2016. By the end of 2017, the total market value grew exponentially to a record high of over $600 billion due to increasing traffic into the cryptocurrency market and a surge in demand mostly from China and Japan. The market has seen growing interest from many institutional investors during this period and the number of initial coin offerings (ICOs) has increased significantly. The trend in the global market capitalization of cryptocurrencies is shown in Figure 2.4. As of Q1 2018, the total cryptocurrency market was valued at slightly more than $400 billion.

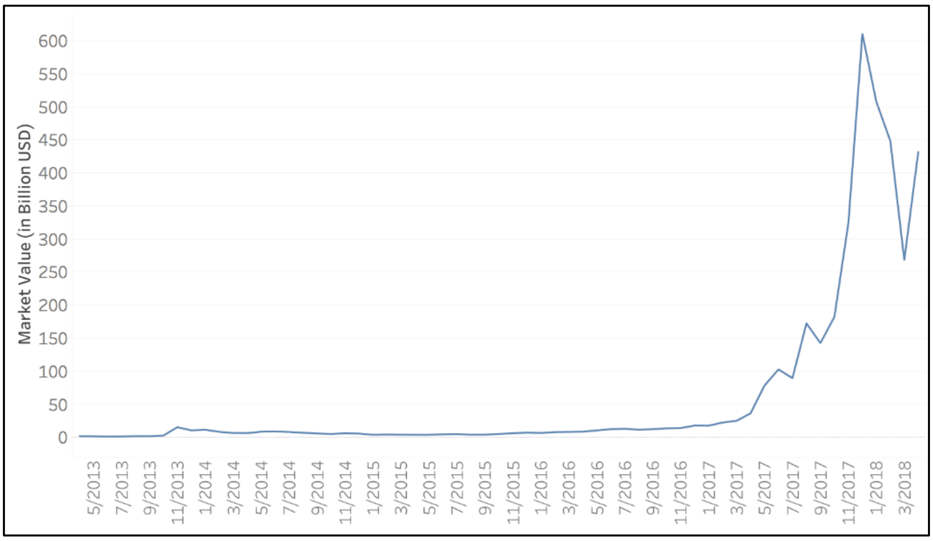


Figure 2.4. Total market capitalization of cryptocurrencies[1].

In the years since the introduction of Bitcoin, numerous other cryptocurrencies have emerged and become part of the cryptocurrency market such as Litecoin, Ethereum, Ripple, Dash, and Monero. Being the debutant in the industry, Bitcoin had enjoyed almost a monopoly with over 70% share of the global cryptocurrency market until early 2017. Slowly, other players entered the market, and, to date, there are more than 1,500 types of cryptocurrencies in operation. Since its inception in 2013, Ethereum has emerged as the main competitor to Bitcoin based on market share. As of April 2018, Bitcoin captures almost 37% of the cryptocurrency market, followed by Ethereum (16%), Ripple (8%), and Bitcoin Cash (6%) as shown in Figure 2.5.

[1] Data source: CoinMarketCap [https://coinmarketcap.com/]. CoinMarketCap is a source for data related to cryptocurrencies' value, their volume and corresponding market capitalization. Data can be extracted through CoinMarketCap's public APIs.

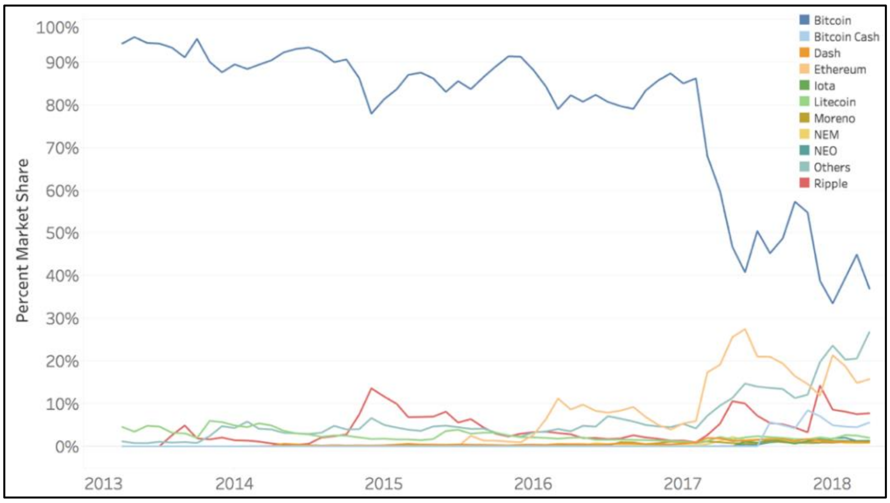


Figure 2.5. Global market share of major cryptocurrencies[1].

Exchanges are an essential component in cryptocurrency transactions. Exchanges are digital trading platforms that offer a marketplace for trading digital assets. Users can buy or sell cryptocurrencies in exchange for conventional currencies or other cryptocurrencies. The cryptocurrencies bought through an exchange are stored in customers' digital wallets. These wallets store the public and private keys required to make a successful transaction of cryptocurrency assets and monitors customers' funds.

The first exchange started to operate in 2010 [6]. By 2018, there were numerous exchanges operating cryptocurrency trades throughout the world. Bitfinex, Bitstamp, MtGox, BTCChina, Huboi, OKChain are some of the popular exchanges in the 2018 market. As shown in Table 2.2, from July 2010 to April 2018, three exchanges, OKChain, Huboi and BTCChina, collectively conducted almost 84% of the total bitcoin trades, whereas, the oldest exchange, MtGox, conducted only 3.3% of trades in Bitcoin's total trade volume. A graphical representation of market share for popular exchanges is shown in Figure 2.6.

Table 2.2. Trade volumes and market share for major exchanges (July 2010 – April 2018)[2].

Exchange	BTC Volume	Market Share
OKChain	586,565,939.90	35.76%
Huboi	544,852,241.80	33.21%
BTCChina	258,007,950.80	15.73%
Mt.Gox	53,861,912.21	3.28%
Bitfinex	45,461,276.87	2.77%
Bitstamp	25,910,946.75	1.58%
Lakebtc	20,767,853.48	1.27%
Bitflyer	15,022,795.60	0.92%
Coinbase	14,915,059.72	0.91%
Others	75,147,603.32	4.58%

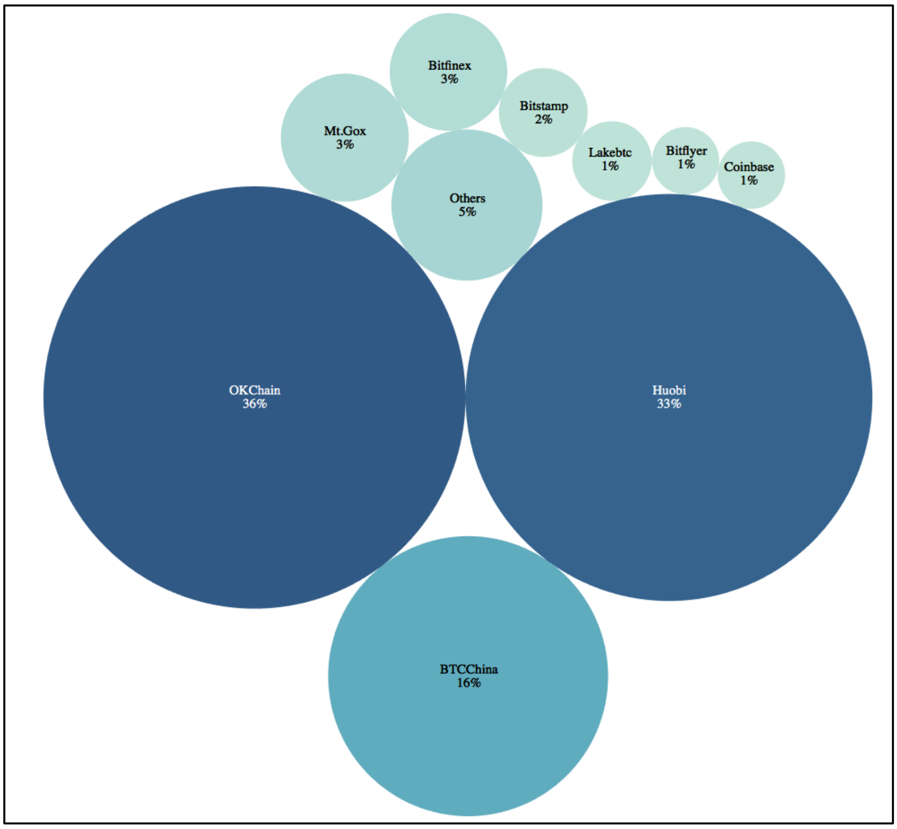


Figure 2.6. Percent of market share for major exchanges (July 2010 – April 2018).

[2] Data source: Data.bitcoinity [https://data.bitcoinity.org/markets/volume/all?c=e&t=b]. This source is managed by Kacper Cieśla, who collects all the data directly from exchanges through their APIs.

3 Protecting Assets

A blockchain is designed to be a secure environment. The use of strong cryptography and secure hashes as security mechanisms enables blockchain to protect digital assets and their transactions from external attacks. The two most important steps to maintain security are: i) to protect a user's private key and ii) secure a user's digital wallet.

3.1 Protecting User's Private Key

Users need to ensure that their private key is stored in a secure way and protected from unauthorized access. If a user's private key were to become known to another entity, that entity could execute transactions while masquerading as the user. The net result is that a user's stolen identity can be used to spend, or otherwise initiate transactions, using the user's cryptocurrency. Consequently, the device that stores the private key needs to be physically secured and strongly password-protected [7].

3.2 Securing User's Digital Wallet

Protecting digital wallets is necessary as the wallet stores digital assets. Measures such as encrypting and maintaining proper backups of the wallet are important. Encryption ensures protection from unauthorized access to the wallet while a backup becomes useful to retrieve the wallet in case the device itself is damaged or stolen. A multi-signature feature that requires a majority of the wallet holders' signatures to approve a transaction can be applied to provide maximum security of a digital wallet. An offline wallet, also known as cold storage, can be maintained to store the majority of a user's assets. As an offline wallet is not connected to a network, it is in no way vulnerable to a network security breach [7].

3.3 Secured but Vulnerable

All systems have vulnerabilities in the real world, and blockchain is no exception. With the ever-growing popularity of cryptocurrency trading, there comes a risk of security breaches and attacks. The cryptocurrency marketplace has experienced several attacks and thefts on exchanges and digital wallets which caused a considerable loss of funds. The largest bitcoin exchange, Mt. Gox, was hacked in early 2014 where bitcoins valued at approximately €460 million were stolen by hackers [8]. This incident forced Mt. Gox to file for bankruptcy. In January 2018, it was reported that NEM tokens worth $533 million were stolen from Tokyo-based exchange Coinchek [8]. Some of the largest Bitcoin thefts are listed in Table 3.1 [9].

Table 3.1. Largest Bitcoin thefts.

Theft	**Timeframe**	**Loss (BTC)**
Bitcoin Savings and Trust	2011–2012	~ 263,024
Silk Road Seizure	Oct-2013	171,955
MyBitcoin Theft	Jul-2011	78,740
Linode Hacks	Mar-2012	46,653
July 2012 Bitcoinica Theft	Jul-2012	40,000
May 2012 Bitcoinica Hack	May-2012	18,548
Allinvain Theft	Jun-2011	25,000
Tony Silk Road Scam	Apr-2012	~ 30,000
Bitfloor Theft	Sep-2012	24,086
Bitomat.pl Loss	Aug-2011	~ 17,000
Bitcoin7 Hack	Oct-2011	~ 15,000
Cdecker Theft	Sep-2012	9,222
Stefan Thomas Loss	Jun-2011	~ 7,000
BTC-E Hack	Jul-2012	~ 4,500
Inputs.io Hack	Oct-2013	~ 4,100
Mass MyBitcoin Thefts	Jun-2011	4,019
Mooncoin Theft	Sep-2011	~ 4,000
Kronos Hack	Unknown	~ 4,000
Bitcoin Rain	2011–2013	~ 4,000
2012 Trojan	Sep – Nov 2012	~ 3,457
Betcoin Theft	Apr-2012	3,172
June 2011 Mt. Gox Incident	Jun-2011	2,643
October 2011 Mt. Gox Loss	Oct-2011	2,609
Andrew Nollan Scam	Feb-2012	2,211
Bit LC Theft	Feb-2013	~ 2,000
Bitcoin Syndicate Theft	Jul-2012	1,853
ZigGap	2012	1,709
Just Dice Incident	Jul-2013	1,300
BTCGuild Incident	Mar-2013	1,254
2012 50BTC Theft	Oct-2012	1,174
Ubitex Scam	2011	1,139
Bitscalper Scam	2012	~ 1,000

4 Transaction Profiling and Scoring Mechanism

Risk is inherent in any transaction. The potential for fraudulent motives on the part of participants or the exchange of stolen goods in a transaction always exists. While certain measures can be taken to reduce such risks, invariably, each party places trust in the other to fulfill their end of the transaction. In order to mitigate this risk, we propose a three-stage solution. First, we create a blacklist of users that are known to be associated with one or more of the major thefts on Bitcoin exchanges. Second, we use classification techniques to profile all transactions based on the potential risk associated with them. Finally, a scoring mechanism is proposed as a measure of trustworthiness at the user level with the aid of the profiled transactions.

4.1 The Blacklist

Blacklisting is one of the primary techniques that organizations use to protect the public from financial scams, malicious web pages, and many other mischiefs on the Internet [10]. For example, SpamCop, an email spam reporting service, uses this approach for listing the IP addresses of entities who send spam. The SafeBrowsing API, a Google service, uses blacklists for listing URLs that lead to malicious web pages. Invaluement, an anti-spam service, employs blacklisting on IP addresses or domain names that are involved in scams.

In our approach, creating a blacklist is the action of grouping entities with whom law-abiding citizens should distrust and avoid making contact. These entities should be known in order to properly educate and protect users. Our blacklist is continuously updated with known fraudulent entities so that users can check before engaging in potentially harmful interactions. Once the entity is found, the scoring mechanism can generate a warning to let the user know that this entity is on the blacklist and cannot be trusted. As such, a blacklist provides the benefit of lookup efficiency [10]. One key limitation of the blacklist is that it operates in a reactive fashion. The list is updated only after an entity has been found to be associated with an illegal activity. However, until then, other entities are vulnerable to the malicious intentions of the criminal entity.

For Bitcoin transactions, a baseline is required to determine which addresses are associated with illegal activities. Certain transactions are linked to criminal activities; hence, the user that made the transaction should not be trusted. Events such as the Mt. Gox hacks, May 2012 Bitcoinica Hack, BTC-E Hack and the Allinvain Theft are all instances in which certain IP addresses were used to commit illegal activities. An address associated with any of these hacks is placed on a blacklist. If a user transacts with one of the addresses on this blacklist, then that user becomes riskier for others to engage in transactions. For example, if User A is associated with the Mt. Gox hacks and User B transacts with User A, then the riskiness associated with doing business with User B increases. The blacklist makes this information publicly available. Therefore, if User C wants to send Bitcoins to User B, they could see that User B has done transactions with the blacklisted User A in the past; this may make User C hesitate to transact with User B.

4.2 Transaction Profiling and Classification

Every transaction has a specific pattern and this pattern recognition is the key to differentiate between "risky" and "non-risky" transactions. Our blacklist plays a crucial role here. We leverage the information gained from past transactions associated with this blacklist and try to identify similarities between new transactions and an established prototype. Any such similarity would explain the new transaction's propensity to be a risky one. Identifying this level of propensity leads to a successful classification of risky and non-risky transactions.

We use a variety of different machine learning techniques that can perform this classification task successfully. Transactions are analyzed based on a set of quantifiable characteristics and are then classified into specific sub-classes with the help of a distance function. A successful profiling largely depends on the degree of accuracy in classification. Once transactions are classified, they are labeled as either of the prototyped classes.

4.3 The Scoring Mechanism

It is often argued that lack of regulations makes the cryptocurrency network vulnerable to fraudulent activities. This prompts us to introduce a scoring mechanism that will enhance trust on cryptocurrency transactions between users. First, a metric in terms of "risk score" has been conceptualized by which a user can gauge the relative potential risk for any future transaction with a fellow user in the network. The risk score, developed at the user level, is defined as a simple ratio of the number of transactions classified as "risky" from a user to the total number of transactions done by the same user. The risk score, denoted by R, is given by the following formula:

$$R = \frac{r}{T} , \tag{1}$$

where r represents the total number of transactions classified as "risky" by a user and T represents the total number of transactions by the same user. As defined, the risk score ranges from 0 to 1 with higher scores indicating a user's higher engagement in risky transactions. If a user's risk score is 0, then this particular user has never been associated with any type of malicious activity involving cryptocurrency. A pictorial explanation of our risk scoring mechanism is displayed in Figure 4.1. In this instance, Dan has the lowest risk score and can be considered the safest user to engage in a transaction with whereas Tim should be avoided because of his extremely high-risk score. Similarly, we can see Bob and Alice are safer entities to transact with than Trudy.

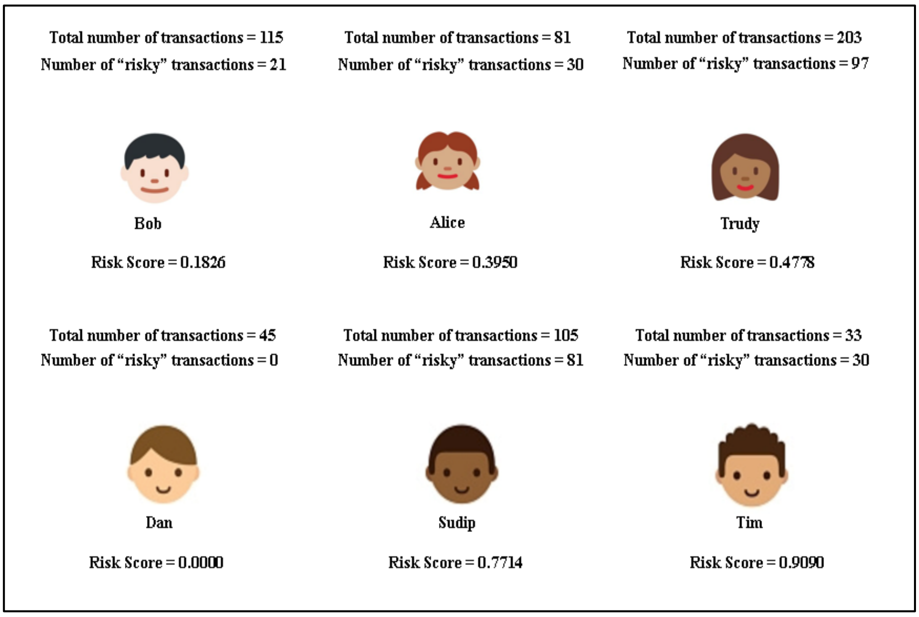

Total number of transactions = 115
Number of "risky" transactions = 21
Bob
Risk Score = 0.1826
Total number of transactions = 81
Number of "risky" transactions = 30
Alice
Risk Score = 0.3950
Total number of transactions = 203
Number of "risky" transactions = 97
Trudy
Risk Score = 0.4778
Total number of transactions = 45
Number of "risky" transactions = 0
Dan
Risk Score = 0.0000
Total number of transactions = 105
Number of "risky" transactions = 81
Sudip
Risk Score = 0.7714
Total number of transactions = 33
Number of "risky" transactions = 30
Tim
Risk Score = 0.9090

Figure 4.1. Risk scoring examples.

This risk score has few limitations. Primarily this scoring method does not define a score for new users, i.e., users with no prior transaction history in a cryptocurrency network. After making the first transaction, a user's risk score can suddenly move up to 1 (the maximum possible value) or go down to 0 (the minimum possible value) given the transaction is classified as "risky" or "non-risky," respectively. Moreover, this scoring mechanism can identify a user with a significantly greater number of "non-risky" transactions as more vulnerable than a user with a smaller number of "non-risky" transactions. For example, if a user has 2 out of a total 50 transactions labeled as "risky", the risk score is calculated as 0.04. On the contrary, if someone makes the first transaction as "non-risky", the corresponding risk score becomes 0, which is better than 0.04. This makes the first user less credible as compared to the second user who is yet to make a considerable footprint in a cryptocurrency network.
To counter these issues with the risk scoring mechanism, we introduce a revised score: a "reputation score". This reputation score, denoted by *S,* is defined as,

$$S = \begin{cases} 0, \ T = 0 \\ T * \left(1 - \frac{r}{T}\right), \ T > 0 \end{cases}, \qquad (1)$$

where *R* represents the total number of transactions by a user, which are classified as "risky" and *T* represents the total number of transactions by the same user. This proposed reputation score has two components: i) risk score (*r*/*T* as previously defined) and ii) the total number of transactions (*T*). This metric ranges from 0 to *T* and provides users the opportunities to start from 0 and build their score with every legitimate (non-risky) transaction. According to this metric, higher reputation scores are better for gauging trust and legitimate business. Table 4.1 shows reputation scores for values of r and T ranging from 0 to 100. Figure 4.2 illustrates different hypothetical scenarios under which a user's risk and reputation score can manifest themselves.

Table 4.1. Reputation scoring.

Total Number of Transactions (*T*)	**Number of Risky Transactions (*r*)**									
	0	1	2	3	4	5	.	.	99	100
0	0	-	-	-	-	-	-	-	-	-
1	1	0	-	-	-	-	-	-	-	-
2	2	1	0	-	-	-	-	-	-	-
3	3	2	1	0	-	-	-	-	-	-
4	4	3	2	1	0	-	-	-	-	-
5	5	4	3	2	1	0	-	-	-	-
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
99	99	98	97	96	95	94	.	.	0	-
100	100	99	98	97	96	95	.	.	1	0

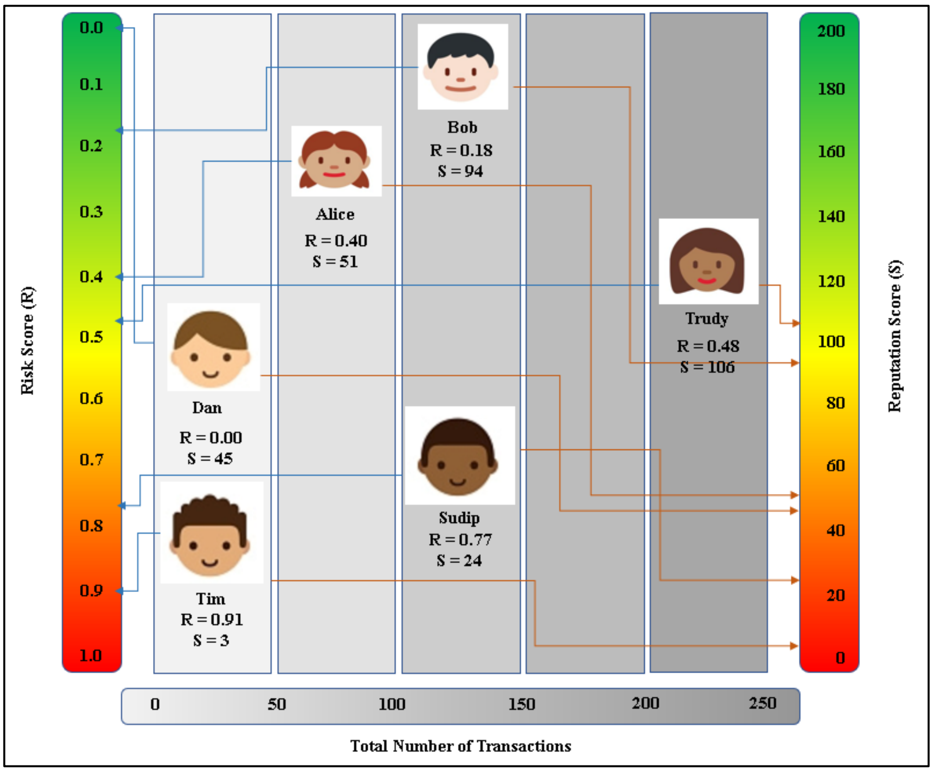


Figure 4.2. Risk and reputation scores for hypothetical users.

5 Blockchain Data

To profile transactions in a cryptocurrency network and classify them based on the potential risk involved, transactional data for Bitcoin with details on the sender, receiver, transaction time and amount are required. For this purpose, we leverage a database on historical Bitcoin transactions from the ELTE Bitcoin Project[3]. This database provides block- and transaction-level details for every Bitcoin transaction recorded through February 9, 2018. The database contains 508,241 blocks and the total number of unique transactions is 303,641,057. We join all attributes together to create a single dataset containing all information without any duplication of information. The attributes are listed in Table 5.1.

Table 5.1. ELTE Bitcoin dataset attribute descriptions.

Attribute	Description	Example
blockID	Unique identifier for each block in bitcoin transaction history	130560
hash	An encrypted hex value for block address	00000000000015b9 b2b91c82f5d95e745 6b754cc188e58
block_timestamp	Current time in seconds calculated based on 1970-01-01-00:00:00 as starting time	1307983943
n_txs	Total number of transactions registered in a block	11
txID	Unique identifier for each transaction	718648
n_inputs	Number of inputs in one transaction	478
n_outputs	Number of outputs in one transaction	2
input_seq	Sequence for inputs in a specific transaction	209
prev_txID	Unique identifier for the previous transaction	718648
prev_output_seq	Previous output sequence for the output prior to the current output	0
addrID	Unique integer value for each address	60412
sum	The total input amount in a transaction which is defined in Satoshis (1e-9 BTC)	5000000000
output_seq	Sequence for outputs in a specific transaction	1
address	Unique identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for payments	1Fq6Ahjkm69zHob ctKCRdGYS25nJir qrLe
userID	Unique identifier for a user	38094

[3] Data source, [http://www.vo.elte.hu/bitcoin/default.htm]. ELTE project was conducted at the Eötvös Loránd University, Budapest, Hungary under the supervision of Prof. István Csabai and Prof. Gábor Vattay. Three PhD students, Dániel Kondor, Márton Pósfai and János Szüle, worked on this project. The objective of this project was to analyze large network datasets to study the navigability of the network of Twitter users and other large-scale studies using Twitter messages.

We assign a risk factor, binary in nature, on the transactions in this dataset. The transactions related to any historical Bitcoin thefts are assigned a risk level of 1 whereas all other transactions are assigned a risk factor of 0. Finally, a sampled set of transactions are selected from the complete and consolidated list of Bitcoin transactions and were considered for analysis and model development. The sampling is designed in such a way that all the historical thefts are selected in the sample and the non-thefts are selected randomly from the transactions without any theft history. This sampling design results in a dataset with a total of 8,109 data points for analysis with 2,172 transactions with risk level 1 and 5,937 transactions with risk level 0.

6 Machine Learning Approach

This section describes several different machine learning approaches that are implemented in order to classify whether a transaction is a risky or not. Three classification algorithms are trained and cross-validated: Random Forest, *K*-Nearest Neighbor, and Support-Vector Machine.

In order to validate our models, the data are split into 80% train and 20% test sets. Then, baseline models are created with all 10 variables: *block_timestamp*, *block_n_txs*, *n_inputs*, *input_sum, output_sum*, *n_outputs*, *output_seq* and *input_seq*. After the baseline models are created, feature engineering is performed in order to fine-tune the models.

6.1 Feature Engineering

Feature engineering is performed after the data are cleaned and ready for model building. In this process, domain knowledge of the data facilitates the development of models with high classification accuracies. Feature engineering guides the researcher in reducing the number of variables that are used as predictors in the models.

6.2 Cross-validation

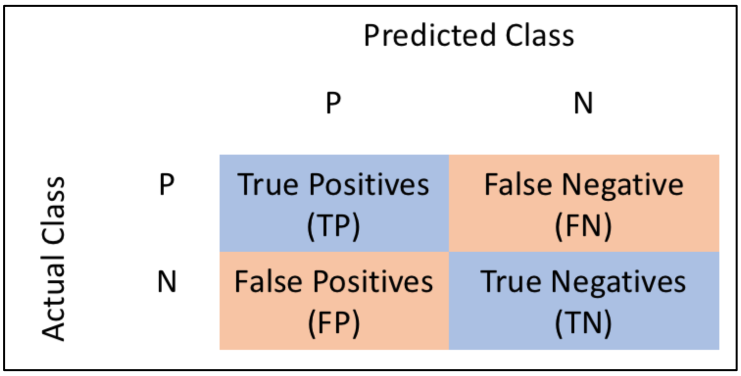
A well-known issue in predictive modeling is overfitting. This refers to over sensitivity of a model toward a specific dataset on which it has been trained. Cross-validation works as a remedy to this issue. This requires the full dataset to be split into two separate subsets, known as the train and test sets. We split our data randomly into an 80:20 ratio for train and test sets. This implies that we train our models on 80% of the observations and validate the models on the remaining 20%.

We use 10-fold cross-validation which returns 10 stratified randomized folds that are made by preserving the percentage of samples for each feature. We use a Stratified ShuffleSplit cross-validator from Python's scikit-learn library for this purpose.

6.3 Model Evaluation

An essential classification model evaluation tool is a confusion matrix. In order to evaluate each model, certain metrics are calculated. The confusion matrix is an *N*-by-*N* matrix, where *N* is the number of classes being classified [11]. The columns and rows of the matrix list the number of instances as actual class versus predicted class, shown in Figure 6.1. The overall accuracy can be calculated as,

$$\frac{TP + TN}{FP + FN + TP + TN} = 1 - Error\,. \tag{3}$$



		Predicted Class	
		P	N
Actual Class	P	True Positives (TP)	False Negative (FN)
	N	False Positives (FP)	True Negatives (TN)

Figure 6.1. Confusion Matrix.

Highlight the issue of overfitting True positives are data points labeled as positive that are actually positive whereas false positives are data points labeled as positive that are actually negative. True negatives are data points labeled as negative that are actually negative whereas false negatives are data points labeled as negative that are actually positive.

Metrics such as precision, recall, F1-score and support are also used to evaluate the performance of a model in predicting unforeseen outcomes. Precision is the proportion of data points that the model assigns as true positives (negatives) that are actually true positives (negatives). It can be calculated as:

$$\frac{TP}{TP + FP}\ \left(\frac{TN}{TN + FN}\right). \tag{4}$$

Recall is the model’s ability to find every data point of interest. It can be calculated as:

$$\frac{TP}{TP + FN}\,. \tag{5}$$

It is important to note that when recall is increased, precision is decreased, and vice versa. When combining precision and recall the result is an F1-score. An F1-score is the harmonic mean of precision and recall which can be given by:

$$2 * \frac{p * r}{p + r} \quad , \tag{6}$$

where p is precision and r is recall. The harmonic mean is used because it strictly deals with extreme values. To create a balanced classification model with the optimal balance of recall and precision, the F1-score should be utilized [11]. Support is the total number of occurrences of each class.

6.4 Random Forest

Random Forest is an ensemble method for classification or regression. We use this method for classification. The Random Forest randomly selects k features from m total features, where $k < m$. Among the k features, it calculates the node d using the best split point. Then, it splits the node into child nodes using the best split. This is repeated until l number of nodes has been reached. Finally, the forest is built by repeating the previous steps n number of times to create n number of trees. The results are obtained by the modal value of categories obtained by individual trees.

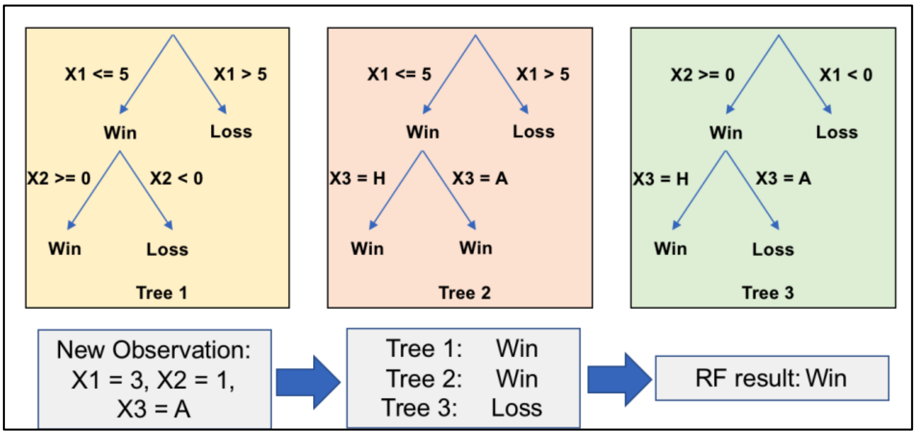


Figure 6.2. Random Forest tree.

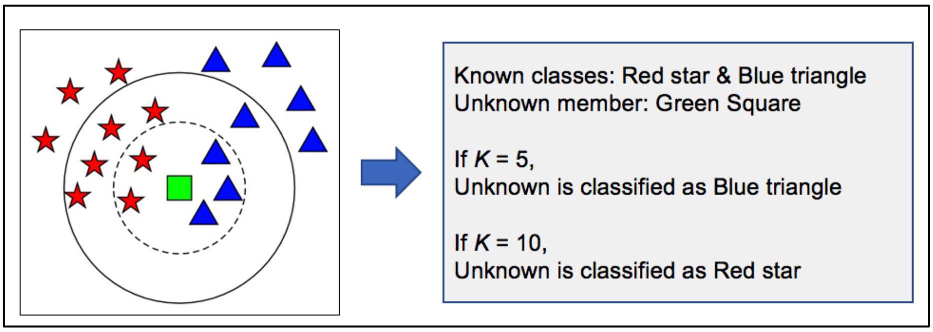
6.5 *K*-Nearest Neighbor

K-Nearest Neighbor (*K*NN) is a non-parametric method for classification or regression. We use this method for classification. In classification, the unknown is classified as the class with the majority of the members. Results of the unknown observation is determined by the average value of the K nearest neighbors of the unknown. K represents the number of data points considered for the classification.

The *K*NN method implements two search types: neighbor search and radius search. When given a set x of n points and a distance function, the search finds the K closest points in x to a single point or set of points y. The distance function used in this paper is the Minikowski distance,

$$d(x,y) = \left(\sum_{i=0}^{n-1} |x_i - y_i|^p\right)^{1/p}. \tag{7}$$

If p is equal to 1, (7) is equivalent to the Manhattan distance; if p is equal to 2, (7) is the Euclidean distance.



Known classes: Red star & Blue triangle
Unknown member: Green Square

If K = 5,
Unknown is classified as Blue triangle

If K = 10,
Unknown is classified as Red star

Figure 6.3. *K*NN classification.

6.6 Support-Vector Machine

Support vector machine (SVM) creates a hyperplane for high dimensional or a set of hyperplanes for classification. SVM uses a "one vs. one" approach for multiclass classification. In a 2-dimensional space, the hyperplane becomes a straight or curved line. The line with the maximum margin forms the support-vector. This approach trains

$$n \times (n - 1) \times 2 = b\,, \tag{8}$$

where n is the number of classifiers and b are the separate binary classifiers. Each binary classifier is trained using examples of two variables that are being classified. The test sample, t, is applied to each of the separate binary classifiers. Then, each binary classifier votes for the variable it is trying to classify. Finally, the test sample receives the label c, where c is the y variable receiving the highest number of votes.

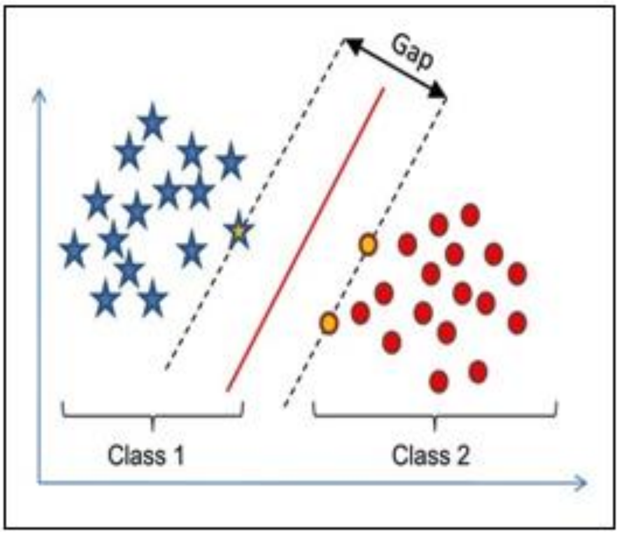


Figure 6.4. SVM classification.

7 Results

In this section, we summarize the results and visualizations of our analyses. The accuracy of each model, a comparison of the models and the split methods are presented. Model performance metrics are displayed to assess how well each method performs in classifying transactions into their respective categories.

7.1 Random Forest Results

We train a baseline model on all 10 variables with an 80% training and 20% for testing split of our data. Table 7.1 displays the Random Forest metrics for the baseline model. This model has a classification accuracy of 100%, as shown in Tables 7.1 and 7.2. Table 7.1 displays the confusion matrix for the baseline model. There were 1,193 observations classified as a non-theft and 429 observations classified as a theft. There are no misclassified observations. This resembles the model accuracy of 100%. Table 7.2 displays the precision, recall and F1-score of the baseline model. These three model performance metrics are 1, which is the highest value possible.

Table 7.1. Random Forest baseline confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,193	0
Actual: 1	0	429

Table 7.2. Random Forest baseline metrics.

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,193
1	1.00	1.00	1.00	429
Average	1.00	1.00	1.00	1,622
Accuracy		100.00%		

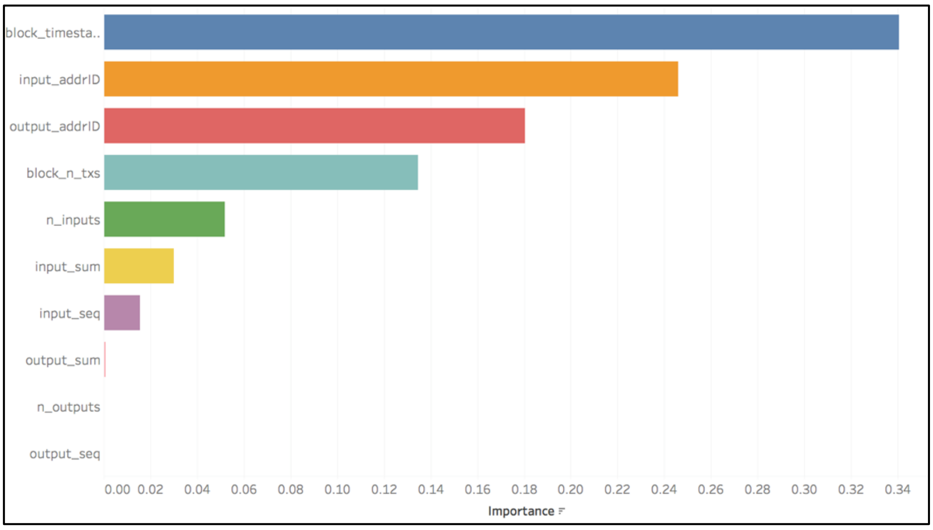


Figure 7.1. Random Forest baseline model feature importance.

Figure 7.1 displays the significant features in the model: *block_timestamp, input_add ID*, *output_addrID*, *block_n_txs*, *n_inputs*, *input_sum*, *output_sum*, *n_outputs*, *output_seq* and *input_seq*. We ran a reduced Random Forest model based on the top 8 features. Variables related to address ID's are dropped from the model as they are used as identifiers. Table 7.3 displays the Random Forest metrics for the second model. This model has a classification average accuracy of 100%, as shown in Tables 7.3 and 7.4. An accuracy of 100% indicates that the algorithm classifies all thefts and non-theft correctly. Table 7.3 displays the confusion matrix for the second model. There were 1,193 observations classified as a non-theft and 429 observations classified as a theft. There are no misclassified observations. This resembles the model accuracy of 100%. Table 7.6 displays the precision, recall and F1-score of the second model. These three model performance metrics are 1, which is the highest value possible.

Table 7.3. Random Forest second model confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,193	0
Actual: 1	0	429

Table 7.4. Random Forest second model metrics.

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,193
1	1.00	1.00	1.00	429
Average	1.00	1.00	1.00	1,622
Accuracy		100.00%		

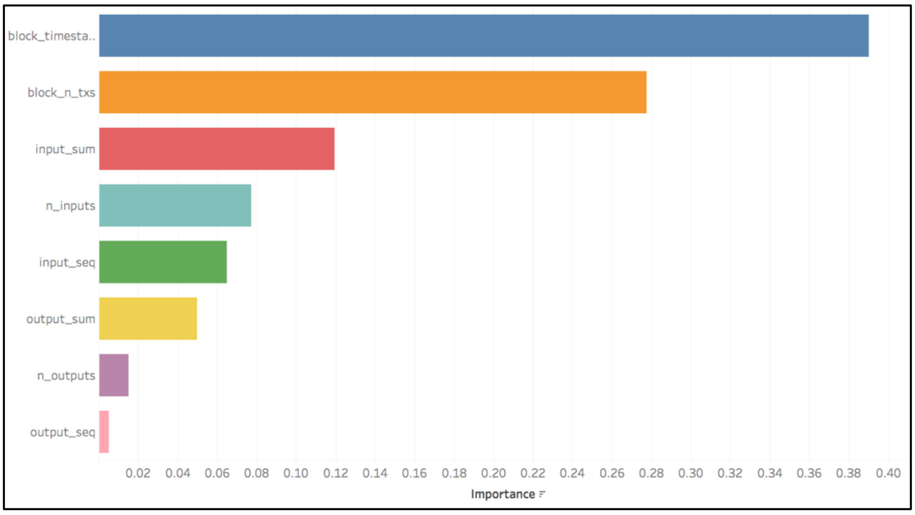


Figure 7.2. Random Forest second model feature importance.

The important features (variables) are displayed in Figure 7.2 for the second model. The variables *block_timestamp*, *block_n_txs*, *n_inputs*, *input_sum*, *output_sum*, *n_outputs*, *output_seq* and *input_seq*. The data are highly skewed towards the number of non-thefts, which can be the reason our model cannot identify the thefts out of all the non-thefts. We further reduce the number of features to 7.

The third model is without *block_timestamp*. Table 7.6 displays the Random Forest metrics for the third model. This model has a classification accuracy of 99.81%. The precision, recall and F1-score of the third model are close to 1. Table 7.5 displays the confusion matrix for the third model. This model misclassifies only 3 out of 1,193 instances where no actual theft occurred. There are no observations misclassified as a theft.

Table 7.5. Random Forest third model confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,190	3
Actual: 1	0	429

Table 7.6. Random Forest third model metrics.

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,193
1	0.99	1.00	0.89	429
Average	1.00	1.00	1.00	1,622
Accuracy		99.81%		

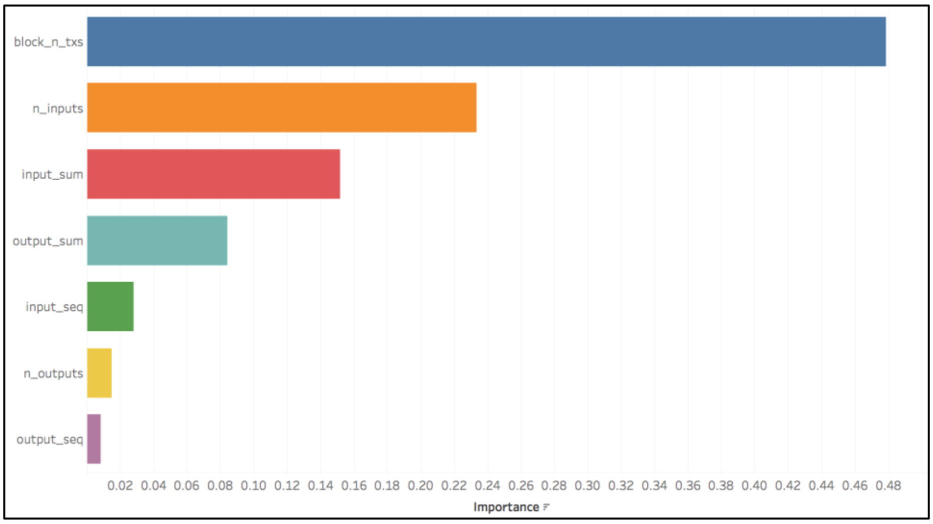


Figure 7.3. Random Forest third model feature importance.

The important features (variables) are displayed in Figure 7.3 for the third model. The variables *block_timestamp*, *block_n_txs*, *n_inputs*, *input_sum*, *output_sum*, *n_outputs*, *output_seq* and *input_seq* are the most important features used in the third Random Forest model.

7.2 *K*-Nearest Neighbor Results

We train a baseline *K*NN model on all explanatory variables with an 80/20 split of the data. Table 7.8 displays the *K*NN metrics for the baseline model. This model has a classification accuracy of 99.96%. Table 7.7 displays the confusion matrix for the baseline model. There are 8 non-thefts that were classified as a theft and 10 thefts that were classified as a non-theft. The misclassifications are minimal for the baseline model.

Table 7.7. *K*NN baseline confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,185	8
Actual: 1	10	419

Table 7.8. *K*NN baseline model metrics.

	Precision	Recall	F1-score	Support
0	0.99	0.99	0.99	1,193
1	0.98	0.98	0.98	429
Average	0.99	0.99	0.99	1,622
Accuracy		99.96%		

To determine the optimal number of neighbors, we iterate through different values of *K* ranging from 1 to 50. Figure 7.4 displays the number of neighbors against the misclassification errors. This reveals the optimal number of neighbors. The optimal *K* is determined by the lowest mean squared error, which happens to be 1 in this case.

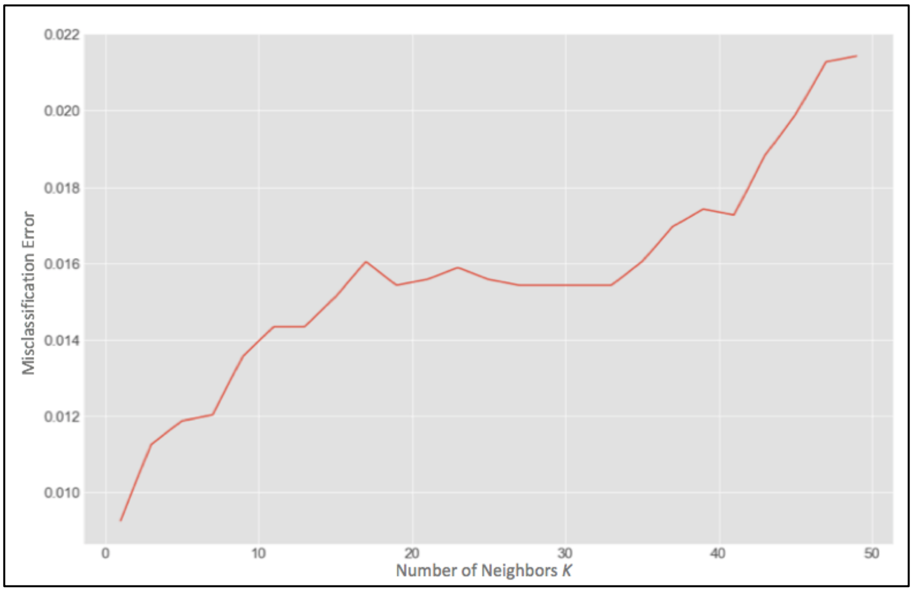


Figure 7.4. Number of neighbors vs. misclassification error.

Once the baseline is established, we perform feature engineering in order to explore how well the *K*NN model classifies with fewer features. The optimal number of neighbors is used along with feature engineering. The second *K*NN model is trained with only 8 features: *block_timestamp*, *block_n_txs*, *n_inputs*, *input_sum*, *output_sum*, *n_outputs*, *output_seq* and *input_seq*. We further reduce the number of features in order to provide a more powerful model.

Table 7.9. *K*NN second model confusion matrix with optimal number of neighbors.

	Predicted: 0	Predicted: 1
Actual: 0	1,184	9
Actual: 1	10	419

Table 7.10. *K*NN second model metrics with optimal number of neighbors.

	Precision	Recall	F1-score	Support
0	0.99	0.99	0.99	1,193
1	0.98	0.98	0.98	429
Average	0.99	0.99	0.99	1,622
Accuracy		98.83%		

Table 7.10 displays the *K*NN metrics for the second model with the optimal number of neighbors. This model has a classification accuracy of 98.83%. The precision, recall, and F1-score are all high, close to 1. There are 9 non-thefts that are classified as theft and 10 thefts that are classified as non-thefts, as shown in Table 7.9.

The third model was trained with only two features: *block_n_txs* and *n_inputs*. Table 7.12 displays the *K*NN metrics for the third model with optimal number of neighbors. With only two features, the third model was able to make correct classifications similar to the baseline and second model. Therefore, *block_n_txs* and *n_inputs* are important in the classification of thefts and non-thefts. This model has a classification accuracy of 98.83%. There are two non-thefts that are classified as thefts and no thefts that are classified as non-thefts, as shown in Table 7.11.

Table 7.11. *K*NN third model confusion matrix with optimal number of neighbors.

	Predicted: 0	Predicted: 1
Actual: 0	1,190	2
Actual: 1	0	427

Table 7.12. *K*NN third model metrics with optimal number of neighbors.

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,193
1	0.99	1.00	0.99	429
Average	1.00	1.00	1.00	1,622
Accuracy		99.88%		

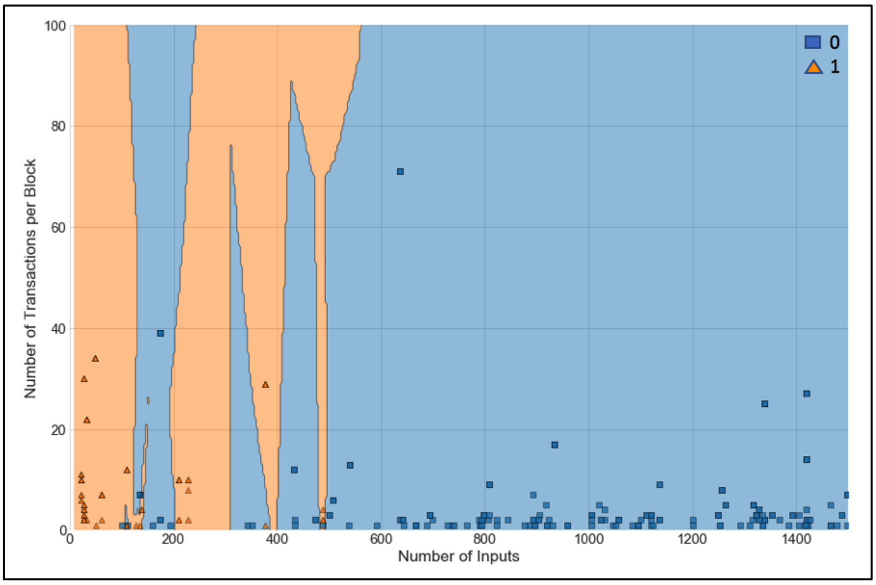


Figure 7.5. *K*NN third model classification results.

Figure 7.5 displays the results of the third model. The orange shaded areas are the thefts and the blue shaded areas are the non-thefts. Likewise, the orange triangles represent the transactions classified as thefts whereas the blue squares represent the transactions classified as non-thefts. Blue squares that lie in the orange shaded area and the orange triangles that lie in the blue shaded area represent the misclassified transactions. This figure displays how well the Random Forest model performed when classifying thefts and non-thefts.

7.3 Support-Vector Machine Results

We train a baseline model on all 10 variables with an 80/20 split. Table 7.14 displays the SVM metrics for the baseline model. This model has a classification accuracy of 97.76%. There are 2 non-thefts that were classified as a theft and no thefts that were classified as a non-theft, as shown in Table 7.13.

Table 7.13. SVM baseline confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,186	2
Actual: 1	0	434

Table 7.14. SVM baseline metrics.

	Precision	Recall	F1-score	Support
0	0.86	1.00	0.92	1,188
1	1.00	0.54	0.70	434
Average	0.89	0.88	0.86	1,622
Average Accuracy			97.76%	

Once the baseline is established, we perform feature engineering in order to explore how well the SVM model classifies with fewer features. A second SVM model is trained with only 8 variables: *block_timestamp*, *block_n_txs*, *n_inputs*, *input_sum*, *output_sum*, *n_outputs*, *output_seq* and *input_seq*. These are the top 8 features in our data set.

Table 7.15. SVM second model confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	1,187	1
Actual: 1	307	127

Table 7.16. SVM second model metrics.

	Precision	Recall	F1-score	Support
0	0.79	1.00	0.89	1,188
1	0.99	0.29	0.45	434
Average	0.85	0.81	0.77	1,622
Average Accuracy			82.66%	

Table 7.16 displays the SVM metrics for the second model. This model has a classification accuracy of 82.66%. There is 1 non-theft that is classified as a theft and 307 thefts that are classified as a non-theft, as shown in Table 7.15.

A third SVM model is trained and tested with only *block_n_txs* and *n_inputs*. Table 7.18 displays the SVM metrics for the third model. This model has a classification accuracy of 85.96%. There are 189 non-thefts that are classified as a theft and 0 thefts that are classified as a non-theft, as shown in Table 7.17.

Table 7.17. SVM third model confusion matrix.

	Predicted: 0	Predicted: 1
Actual: 0	999	189
Actual: 1	0	434

Table 7.18. SVM third model metrics.

	Precision	Recall	F1-score	Support
0	1.00	0.84	0.91	1,188
1	0.70	1.00	0.82	434
Average	0.92	0.88	0.89	1,622
Average Accuracy		85.96%		

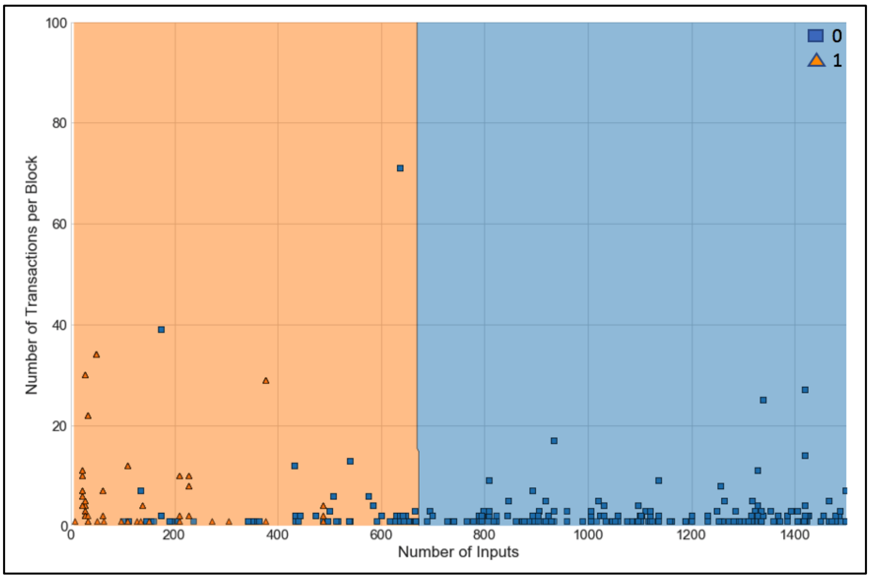


Figure 7.6. SVM third model classification results.

Figure 7.6 displays the results of the third SVM model. The orange shaded areas are the thefts and the blue shaded areas are the non-thefts. The orange triangles represent the thefts classified values whereas the blue squares represent the non-theft classified values. Blue squares that lie in the orange shaded area and the orange triangles that lie in the blue shaded area represent the misclassified transactions. This figure displays how well the Random Forest model performed when classifying thefts and non-thefts.

7.4 Model Comparison

In our study, we have used machine learning techniques to classify transactions based on their propensity of risk. We start with a baseline model with all relevant features followed by reduced models trained with key features selected from the baseline model. Both the Random Forest and *K*NN methods provide almost a perfect classification for the baseline model as well as the reduced models. Our reduced models are built based on the top 8, top 7 and top 2 features identified from the baseline Random Forest model. None of these models have misclassified a risky transaction as a non-risky one.

The accuracies and F1-scores for all these models are presented in Figure 7.7 and Figure 7.8, respectively. The models with the least number of features are preferred, as they are easier to interpret. Random Forest and *K*NN have achieved more than 98% accuracy, regardless of the number of features considered in the model. On the contrary, SVM is dependent on the number of predictors. The accuracy for SVM has dropped from 98% to 83% when 8 of the 10 predictors are selected. The baseline model misclassified two of the non-risky transactions but classified all risky transactions correctly whereas the top-8 model fails to capture risky transactions in 70% of cases, 307 times out of 434 in total.

The drop in accuracy prompts us to retrain SVM based on the top 2 important predictors: *block_n_txs* and *n_inputs*. This SVM model provides a realistic classification accuracy of 86%. This model gives a high F1-score of 0.89. An increased accuracy level with fewer predictors indicates the presence of factors that have a negative influence on the classification.

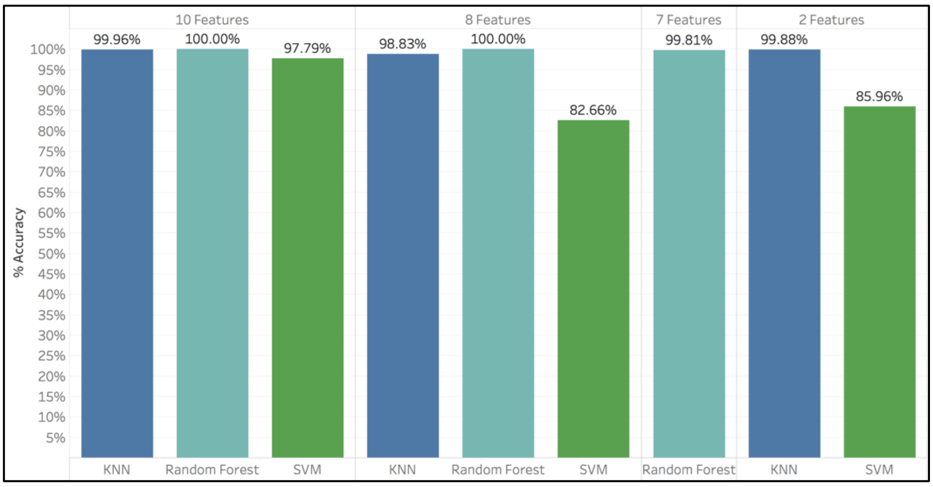


Figure 7.7. Model comparison for accuracy.

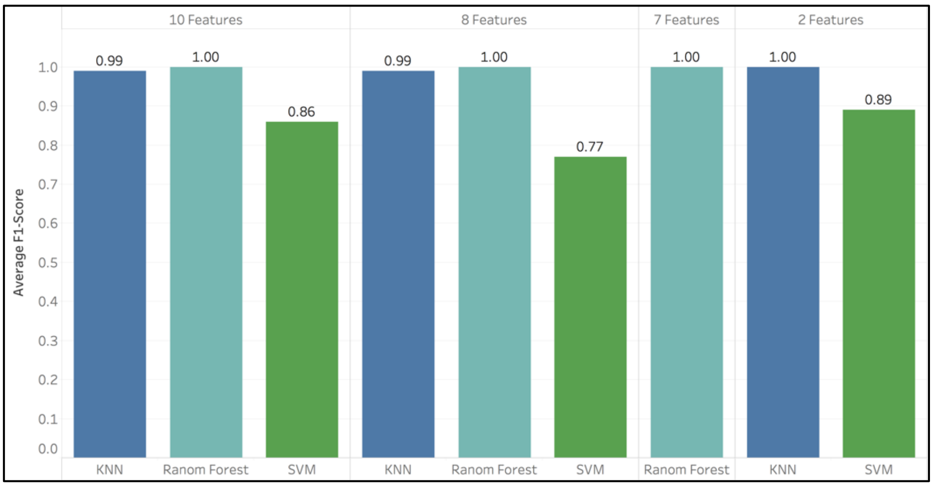


Figure 7.8. Model comparison for F1-score.

8 Ethical Discussion

The Association for Computing Machinery's (ACM) code of ethics contains 24 imperatives by which all professionals should adhere [12]. Among them, "Avoid harm to others" and "Respect the privacy of others" are arguably the most relevant to trust in cryptocurrency transactions.

Our reputation scoring methodology has the potential to do harm to law-abiding cryptocurrency users. No machine learning model is 100% accurate. As a result, our machine learning models can overstate a user's frequency of transactions with entities associated with a theft of an exchange. This would make other users less likely to engage in transactions with such a user, despite the user's non-malicious intentions and perfectly legal transactions. Consequently, undue harm would be caused to that user by restricting their ability to do business in the marketplace.

Additionally, our approach arguably restricts the privacy of cryptocurrency users. Trust in the presence of anonymity requires an examination of the company users keep. By developing and publicizing a reputation score for each user, we are revealing information about their association with individuals or entities that engage in unlawful activities. While the identity of each user is not explicitly disclosed, a single number that represents one's reputation score, on the surface, says much about the parties – whether good, bad or neutral – with which a user makes transactions. This privacy concern becomes especially salient if a user would prefer not to share the identities of the users they have transacted with in the past. After all, it is the right of an individual to conceal most types of personal information from the general public.

The publication of a reputation score, such as the one we present, generates additional questions that may have not come to light previously. For example, would a cryptocurrency user have the option to “opt out” of their reputation score being viewable by all other users? If so, how many users could realistically be expected to remove their public key from the risk scoring list? If the vast majority of users opt out, that severely reduces the usefulness of the risk scoring concept. If users are not given opt-out opportunity, that raises the concern of the aforementioned privacy restriction. Moreover, who or what would be in charge of storing and managing our reputation score database? If an independent third-party is responsible, would that undermine the decentralized nature of the cryptocurrency marketplace? These are just some of the many questions that would need to be carefully answered before our reputation scoring methodology could be ethically and practically implemented in the marketplace.

9 Conclusions

Based on the available Bitcoin transactions, we implement a successful classification mechanism to differentiate risky transactions from non-risky ones. A successful classification leads to a reliable scoring mechanism. Our reputation scoring mechanism, which is practical and easy to calculate, is a foundation for enhancing trust in the cryptocurrency marketplace. After transactions are classified, all the users identified by their respective public keys are assigned a reputation score based on their involvement in risky transactions from their full transaction basket to date. Consistent legitimate transactions of cryptocurrency assets provide ample opportunity for users to build a credible reputation over time. However, this reputation can be damaged with their frequent involvement in risky transactions. Users meeting a certain transaction threshold with a low reputation score are blacklisted. The blacklist, updated continuously, works as a guideline for making safe Bitcoin transactions.

The success of a financial transaction depends largely on trust which can be ensured by the users on either side of a transaction. In a cryptocurrency marketplace in which intermediaries are non-existent, a self-attestation mechanism in the form of a reputation score offers a viable alternative to enhance trust. It empowers users with the ability to carefully consider others before transacting with them.

10 Future Work

In our present solution, we develop a reputation scoring mechanism that is predominantly built on the characteristics of transactions. The ever-changing nature of human behavior is reflected in users’ transactional patterns. This requires a continuous monitoring of our classification models to accommodate the necessary amendments based on the ongoing inflow of data.

Anonymity in blockchain is a double-edged sword. The current mechanism is not able to track whether a criminal purposefully creates multiple dummy transactions to improve their reputation score. Moreover, multiple user ID’s by the same user are also approved in the current structure of the blockchain network. This creates a further opportunity for criminals to take advantage of their anonymity. We aim to replace our scoring metric with a more sophisticated one in the future to address these limitations. Blacklisting the stolen coins is another action suggested in this regard.

This work may also be extended to study the impact of additional factors such as whether a transaction is pooled or an exchange in our classification of transactions into risky or non-risky categories. A pooled transaction is of a newly minted coin that goes to the same input address. These types of transactions can be identified by the output location. Typically, an exchange transaction will have an output to some third-party website. The website matbea.net is a popular source from which to collect this information.

Educating participants in cryptocurrency transactions on the advantages of our reputation scoring approach is key for blockchain-based marketplaces to become more trustworthy in the future. While adoption will undoubtedly be slow, pilot testing of our method on real-world cryptocurrency transactions would allow entities to gauge how effective our reputation scoring mechanism is in empowering users with a self-guided trust. An advanced analysis to quantify the impact of this scoring mechanism in cryptocurrency marketplaces would reveal further possible improvements with a viable go-to-market solution for the industry.

References

1. L. D. Brandeis, “Other People’s Money and How the Bankers Use It”. Frederick A. Stokes Company: New York. Originally published in Harper’s Weekly. Page 92. [Online]. Available: http://www.law.louisville.edu/library/collections/brandeis/node/196.
2. T. Culpan, “$2.3 Billion in Losses Highlights Crypto’s Moral Hazard”, 2018, [Online]. Available: https://www.bloomberg.com/view/articles/2018-06-11/-2-3-billion-in-losses-highlights-crypto-s-moral-hazard
3. D. Ron and A. Shamir, “Quantitative Analysis of the Full Bitcoin Transaction Graph”, [Online]. Available: http://arimoto.lolipop.jp/584.pdf
4. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. Published in 2008 on Bitcoin.org [Online]. Available: https://bitcoin.org/bitcoin.pdf
5. Statista, "Number of Blockchain Wallets 2018" [Online]. Available: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/
6. Dr. G. Hileman, M. Rauchs, University of Cambridge – Judge Business School “Global Cryptocurrency Benchmarking Study”. [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
7. Trustis, "Private Key Protection", 2010, [Online]. Available: http://www.trustis.com/pki/bat/guide/private-key-protection.htm#Contents
8. Coindesk, "Coincheck Confirms Crypto Hack Loss Larger Than Mt.Gox," [Online]. Available: https://www.coindesk.com/coincheck-confirms-crypto-hack-loss-larger-than-mt-gox/
9. Bitcoin Forum, "List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses," [Online]. Available: https://nxtforum.org/pub-crawl/list-of-major-bitcoin-heists-thefts-hacks-scams-and-losses/?PHPSESSID=hdb8b2rr90cadm6kflprmi35a2
10. M. Felegyhazi, C. Kreibich, V. Paxson, “On the Potential of Proactive Domain Blacklisting”. Published on the International Computer Science Institute. [Online]. Available: https://www.usenix.org/legacy/event/leet10/tech/full_papers/Felegyhazi.pdf
11. D. Lary, "Supervised Classification", 2018.
12. ACM Council, “ACM Code of Ethics and Professional Conduct”, [Online]. Available: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct