Secure Lending: Blockchain and Prospect Theory-Based Decentralized Credit Scoring Model

Vikas Hassija , Gaurang Bansal, *Member*, *IEEE*, Vinay Chamola, *Member*, *IEEE*,
Neeraj Kumar, *Senior Member*, *IEEE*, Mohsen Guizani, *Fellow*, *IEEE*

***Abstract*—Credit scoring is a rigorous statistical analysis carried out by lenders and other third parties to access an individual's creditworthiness. Lenders use credit scoring to estimate the degree of risk in lending money to an individual. However, credit score evaluation is primarily based on a transaction record, payment history, professional background, etc. sourced from different credit bureaus. So, evaluating a credit score is a laborious and tedious task involving a lot of paperwork. In this paper, we propose how blockchain can provide the solution to decentralized credit scoring evaluation and reducing the amount of dependence of paperwork. Lending money is not always objective but subjective to every lender. The decision of lending involves different levels of risk and uncertainty, depending on their perspective. This paper uses the prospect theory to model the optimal investment strategy for different risk vs. return scenarios.**

***Index Terms*—Blockchain, Behavioural Economics, Credit Score, Prospect Theory, Security, Fin-tech.**

I. Introduction

Lending money is risky but at the same time, is a very crucial source of income for banks, investors, and financiers. To minimize the risk of lending and to calculate the probability of a borrower of becoming delinquent, the most common method being used since the 1950s is credit scoring [1]. This method of calculating a credit score is based on some statistical analysis of historical data, which is very common in both consumer lending and mortgage lending.

A diversified set of data including the age of the applicant, sex, purpose of the loan, previously submitted applications, previous loans completed, job type, duration in a job, housing type, bank account average balance, and previous defaults are used to calculate a fair credit score. All such data goes through multiple cycles of statistical analysis to create an individual's scorecard. An acceptable model of credit scoring is expected to give a high score to the applicant whose loans are expected to perform well and a low score to the applicants who are more likely to become defaulters. The complexity of analysis involved in calculating the actual credit risk is quite tedious. Hence, there have been various visual analytic systems and software created to make the analysis and correlation easier [2, 3].

Vikas Hassija, Gaurang Bansal and Vinay Chamola are with the Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India 333031 (e-mail: vikas.hassija@gmail.com,h20140128@pilani.bits-pilani.ac.in, vinay.chamola@pilani.bits-pilani.ac.in).

Neeraj Kumar is with the Department of Computer Science, Thapar University, Patiala, India 147004 (e-mail: neeraj.kumar@thapar.edu).

Mohsen Guizani is with the Department of Electrical and Computer Engineering, Qatar University, Doha (e-mail: mguizani@uidaho.edu).

However, the evaluation of credit scoring is quite slow, owing to the complexity of task aggregation and computation. The first reason for the delay is that there is a diverse set of borrowers for business loans. This makes it difficult to develop an accurate model for credit scoring. For example, it is observed that some malicious accounts received higher scores in comparison to genuine accounts because of a lack of proper transaction history, which came to be known later. Second, a major portion of the applicant data is collected from the lenders who previously provided loans to them and from various third parties involved in credit scoring. So there is a dependency on credit bureaus, and this model assumes that this dependency can never be compromised. Third, the scores are highly volatile and change for different trusted authorities depending on the information available to them. The most common credit score used by 90% of the lenders is the Fair Isaac Corporation (FICO) score ranging from 300-850 [4]. The FICO score of an individual is based on the credit data, including credit usage, credit types, length of credit history, payment history, and the recent credits received. FICO scores are calculated by the three credit bureaus, namely Equifax, TransUnion, and Experian.

Another problem with the current models for credit score evaluation is that they do not take into account the behavioral models of lenders [5], [6]. The decision of lending based on credit score is always subjective to every lender. The decision of lending involves different levels of risks and uncertainty, depending on their perspective. The information processing method for humans is quite different and illogical as compared to machines. Humans are loss-averse. Losses are interpreted differently than the equivalent gains by the lenders. Losses are disliked more than the equivalent gain, and the amount of risk one is ready to take to avoid a loss is more than the risk one can take to earn an equivalent gain.

This paper discusses how blockchain can provide a solution to the above-mentioned problems by eliminating the need for third-party verification [7]. Fig. 1 shows the proposed model where the credit scoring mechanism is achieved through a blockchain distributed ledger technology. The proposed model of blockchain is a consortium or federated blockchain network where all the lenders and borrowers can enter the the network at any time by providing their identity. All the transactions are encrypted using asymmetric key cryptography to maintain the privacy of the user data. Only the intended borrowers can view and verify the user details using their private key. The transactions are digitally signed by the users using their private key to prevent the issues related to non repudiation.

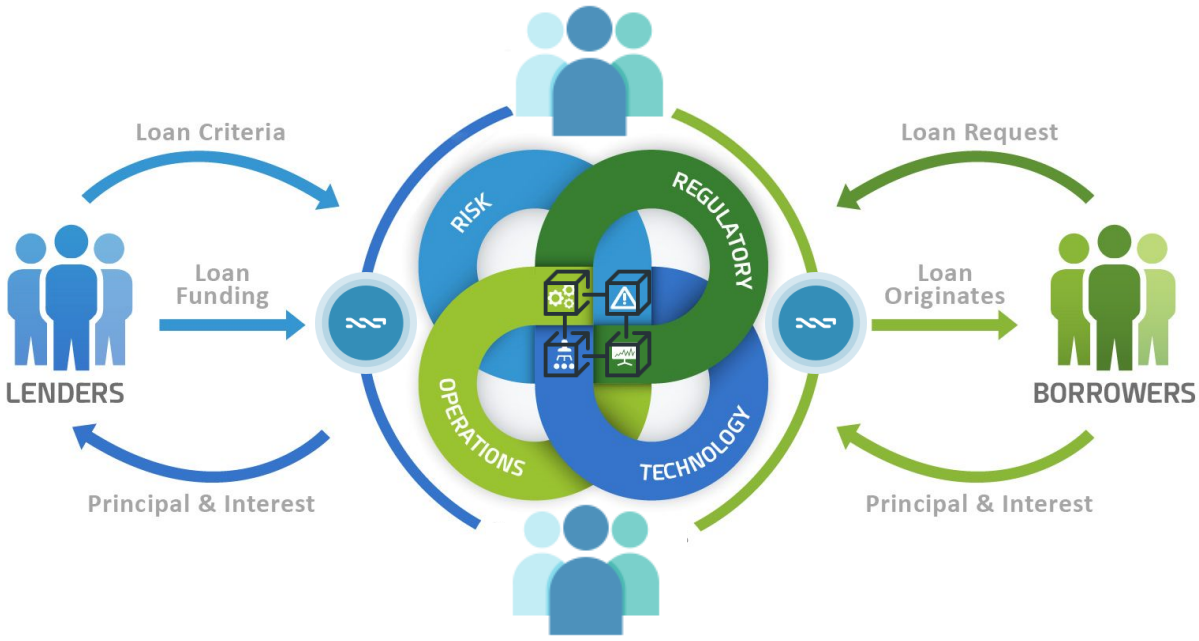

Fig. 1: Proposed credit scoring model using blockchain. All transactions are verified and saved in a distributed ledger which can be used by lenders for credit score evaluation. The difference between the traditional and our approach is that there are no intermediaries or third parties required.

All the lenders can have a consensus credit scoring value. This model takes into account the transactions, risks, and returns that are available for investors and/or lenders. It also ensures transparency of all the activities along with providing privacy and anonymity for all individuals.

In this paper, we also take into account the behavior modeling of different lenders based on their perspective and different borrowers by using Prospect Theory [8].

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 illustrates the proposed scheme. Section 5 discusses the need for a prospect theory model and evaluation of parameters used for the credit scoring evaluation. Section 4 discusses the investor's viewpoint of the computed credit score. Section 6 discusses the results and analysis. Finally, Section 7 concludes the article.

In this paper, we employ a common consensus platform for all the lenders to come to a unified credit score value. We also use the behavioral model for lenders in lending money based on the credit score. The major contributions of this paper are as follows:

- **Decentralized & unified credit score evaluation**
  Providing a decentralized and unified mechanism for credit score evaluation using blockchain. Every transaction is recorded and is immutable.
- **Behavioural Modelling for lenders**
  Using prospect theory, we model the trade-off between risk and return for lenders based on decentralized credit scoring.
- **Reducing dependency on data sources**
  The availability of immutable public ledger removes dependence on different data sources and loss of transaction information.

II. Related Work

This section describes the existing work for credit scoring evaluation and behavioral modeling for lenders. Authors in [9, 10, 11] present statistically-based machine learning models used for calculating the credit scores. They proposed different ways to define the weights of each parameter and fine-tune them depending on different scenarios. A detailed survey of various machine learning algorithms used for calculating a fair credit score is presented in [12]. A negative Rank model is presented in [13] to calculate the credit score of various merchants by collecting the survey from the purchasers in a secure and privacy conserving manner.

In [14], Gaonkar and Viswanadham discussed the credit risks involved in supply chain management. A strategic, operational, and tactical approach to handle credit risks is also explained. Authors in [15, 16, 17] present a decision support and fuzzy logic approach for credit risk assessment for private firms. Various data mining methods, such as neural networks, decision trees, and logic regression, are used to calculate the risk involved in a particular loan. Roman and Stefano introduced a Trusted Data Marketplace (TDM) in [18]. Their objective was to solve the problem of limited data sharing due to the lack of trust between the individuals and third parties. Credit score depends on more than just the bank history. Authors in [19] changed the parameter of credit score evaluation by making it more dynamic and closer to one's social perspective. They evaluated the credit score by

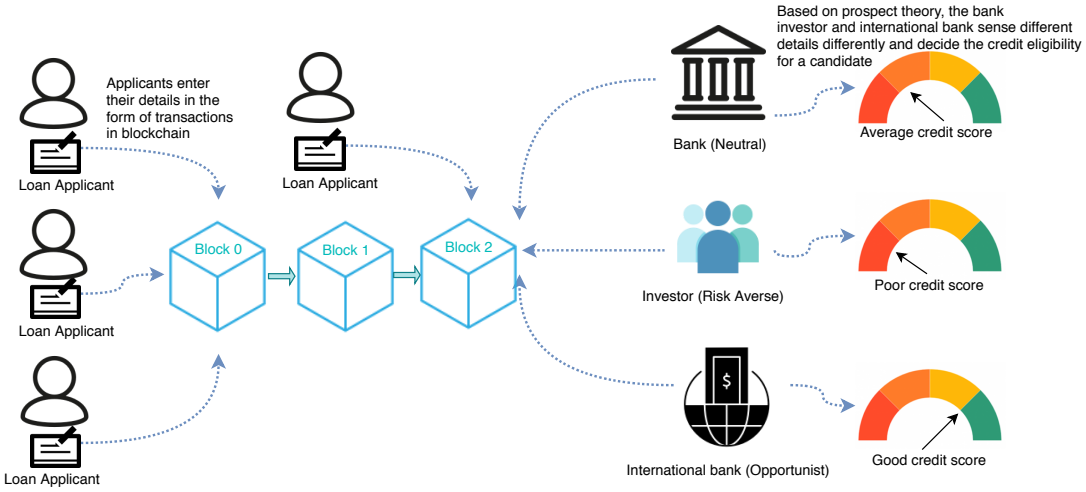

Fig. 2: Secure Lending Model

quantifying the data using a person's social media content. A further enhancement of this research was to understand a person's social status. The solution is an application that draws information through Short Message Service (SMS). This data is quantified, and then a credit score is evaluated.

Using a centralized system to calculate the credit scores is associated with various issues. The customer's data is used by the giant companies to calculate the credit score, and the individual has no control over who gets to see the credit data of an individual. The blockchain is a powerful decentralized peer-to-peer platform where the individual can control its data and its visibility [20, 21]. Every individual who becomes a part of the decentralized network for a credit score calculation can participate in the process. All the records added to the chain are connected to the previous entries, and an update on the chain requires a multi-level verification [22]. The current data storage or centralized servers with the bureaus is highly susceptible to security breaches. Equifax data was breached in 2017, and that breach impacted 148 million customers compromising information like Social Security numbers, names, addresses, and tax ID information [23]. Bloom is an organization that creates a framework for credit scoring using blockchain. Only the lenders who are authorized by the individuals can view and verify the data of the individuals [24]. The framework does not cater to the individual demands of the lenders and investors, as done in the proposed model. The smart contract feature of blockchain is not used in bloom. The basic concept of credit score calculation is kept the same, and only the architecture is shifted from centralized to distributed. The proposed model uses prospect theory in a smart contract to understand the acceptable risk level of each lender and thereby provides an individualistic credit score of a user for a different type of lenders.

Another issue with the traditional credit scoring mechanisms is the process itself. It relies heavily on previous loan repayment, which is an obvious problem for the 3.5 billion unbanked and under-banked people across the globe who lack access to formal financial institutions and, by default, to loans [25]. Blockchain is a decentralized application can be used by any individual for microloans and can make the unbanked individuals participate in the formal financial system. Colendi is a decentralized platform for credit scoring, that uses over 1,000 unique indicators to provide a credit score to the unbanked individuals in a secure manner [25].

Lending money depends on the best possible trade-off between return and risk. Markowitz proposed the Modern Portfolio Theory [26], where the portfolio is the creditworthiness of customers for lending. The theoretical background for the relationship between return and risk is provided in that theory. Return, and its standard deviation is combined by the efficient portfolio. Portfolio choices are determined under a certain degree of uncertainty using the Expected Utility Theory (EUT). Outcomes using objective probabilities are evaluated by investors who are uniformly risk-averse under EUT.

Instead of individual probabilities, Quiggin [27] distorted the cumulative probabilities of ranked outcomes. Cumulative Prospect Theory was developed by Tversky and Kahneman to overcome inconsistencies with first-order stochastic dominance [28]. A portfolio optimization method based on cumulative prospect theory is presented in [29].

The behavioral modeling for lenders does not account for financial phenomena, different risk attitudes, diminishing sensitivity, and loss aversions such as the paradoxes of Allais and Ellsberg [30]. Daniel Kahneman and Amos Tversky in 1992 came up with prospect theory in cognitive psychology that describes how people choose risk involving probabilistic alternatives where probabilities of outcomes are not certain. For their contribution, they received the Nobel prize in 2002.

III. Proposed System Model

The current credit scoring system completely relies on a handful of central organizations that store all the user data and calculate the credit scores. The credit information of the borrowers is frequently in transit, and it opens us up to security risks. Using blockchain, we can go on saving all the transaction data in a single chain that is distributed to all the customers and lenders. Everyone can validate the data on the chain, but no attacker can tamper the data ones committed.

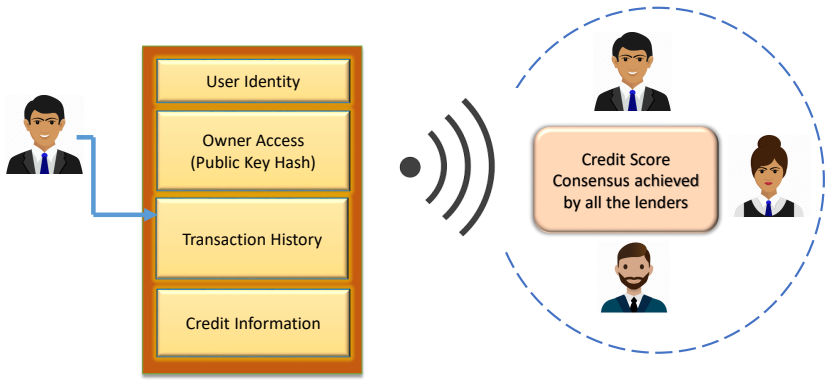

Fig. 3: Description of the block created. The block is propagated to all the nodes.

In this section, we present the detailed system model, design goals, and security assumptions in the proposed model.

A. Digital Identity

In the case of a new user, a unique address is generated for the network, and two keys, namely − private and public key are generated from a key generation algorithm (KGA) [31, 32, 33]. Two random and large prime numbers p, q are chosen in a way that $k = p * q$. Further, an integer (b) is chosen from $\left[1, \phi(k)\right]$ where $\phi(k)$ is the Euler function. The great common multiple of b and $\phi(k)$ is 1 [34, 35]. Now, to generate the public and private keys, KGA calculates a new parameter g, such that $g * b = 1(modk)$. Ones this is done, b is assigned as the private key, and g is assigned as the public key of a user [36, 37]. The public key is unique to the user [38].

1) Block: Blockchain consists of a sequence of blocks. Each block, as shown in Fig. 3 contains a cryptographic hash value, the timestamp of the transaction, Merkle tree root, transaction information, and previous block hash value [39, 40]. The size of the transaction and the predefined size of a block dictates the number of transactions to be included in a block. The use of cryptographic hashing and hash chaining makes it difficult for an adversary to tamper the information that has been already committed on the chain [41]. Everyone on the network can check the transactions that are committed, but no one can change the transaction data [42, 43].

2) Digital Signature: The problem of non-repudiation is prevented by attaching every transaction with the digital signature of the owner. In asymmetric key cryptography, a key is divided into two parts, a private and a public key [44]. An owner can sign the transaction using his private key, and everyone on the network can verify the transaction using the public key of the owner.

B. Consensus Algorithm and Mechanism of Adding a Block

We design a network model with multiple numbers of ordinary users, banks, and credit bureaus. Let B_n be the number of banks or investors or lenders, U_n be the number of ordinary users, and A_n be the number of agents or bureaus who are assigned the task of calculating the credit score. There is another set of entities in the network termed as P_n, i.e., prospective bureaus. The Agents gather the information from the ordinary users and calculate the credit score that is used by the respective banks to decide upon the eligibility for loans.

The consensus is a way of reaching an agreement between the nodes. As the transaction, once added to the block, cannot be modified ever again, it needs to be verified the first [45]. In a traditional system, third parties like banks ensure that every transaction is verified and legit. In a peer-to-peer system, there is no governing authority for the same. In the blockchain, to overcome Byzantine problem [46] among the nodes, there are various consensus protocols [47].

We use the proof of voting algorithm to reach a consensus in terms of the credit score being calculated. We consider the fact that a single bureau or a set of bureaus can become malicious, and therefore, the model does not rely on the score calculated by a bureau until it gets a positive vote from more the 50% of the banks in the network. Also, we define a concept of a periodic cycle, and a single bureau is allowed to calculate the credit score only for a single cycle. In every cycle, the new set of bureaus is assigned the task of score calculation based on the votes they receive from the banks in their previous periodic cycle. A set of bureaus is randomly selected initially, and the bureaus start gaining a higher vote and thereby a higher probability of getting an opportunity of creating further blocks. A round of consensus is considered to be completed only when a new block is generated. If a bureau fails to create a block in a pre-defined time interval, then the responsibility of mining the block goes to the next prospective bureau. A block must have more than 50% of votes from valid lenders for a block to become valid. The network can finally reach a consensus if at least one bureau normally works. This prevents the issue of forking as it happens in the traditional POW consensus. The block, thus created, is shown in Fig. 3.

C. Security Analysis and Assumptions

The credit information of a user is highly confidential and private. A robust security analysis is required to prevent the

leak of any user information in public. The public blockchain networks such as bitcoin and ethereum maintain the anonymity of the data on the blockchain. However, completely anonymous data would not be useful for the lenders and credit score bureaus, as the credit score cannot be anonymous. Typical bitcoin transactions can be kept entirely anonymous as such networks are only concerned with the balance in a particular account and prevention of the double-spending problem. The credit scoring blockchain is concerned with the credit score of a particular individual, and a completely public blockchain cannot function in this case as required. Therefore, we propose a consortium or federated blockchain network, where users are are required to submit their identity proof before they enter into the network. Although the identity is submitted, it is encrypted using the public key of the authorized lenders and digitally signed using the private key of the user. The cryptographic algorithms help in providing the features of authorization and anonymity simultaneously. For normal users, the transactions are transparent and anonymous as in public blockchain, and for authorized lenders, the transactions are authorized by the identity of the users. The issue of preventing low-credit users from entering the network with new anonymous identities is also solved using the consortium network. The users need to get authorized suing their identity documents before they are allowed to enter the network. We assume that the lenders and borrowers are providing genuine information about their needs.

IV. Need of Prospect Theory & Parameters for Credit Score Evaluation

When a lender receives a loan application, based on the borrower's profile, the lender has to make a decision regarding whether to go ahead with the loan approval or not. Two types of risks are associated with the decision:

1) If the applicant is a good credit risk, i.e., is likely to repay the loan, then not approving the loan to the person results in a loss.
2) If the applicant is a bad credit risk, i.e., is not likely to repay the loan, then approving the loan to the person results in a financial loss.

The prospect theory model incorporates a value function that represents how lenders value things. For every investor is utility gain for investor or return parameter, while is the risk or loss parameter captures loss aversion. This is one best behavioural model that exists and has been awarded Nobel Prize. **Prospect theory is a theoretical model and can be implemented as allocation optimisation problem.**

It may be assumed that the second risk is a greater risk, as the lender had a higher chance of not being paid back the borrowed amount. So it's on the part of the lender to evaluate the risks associated with lending money to a customer. This study aims at addressing this problem by using the applicants demographic and socio-economic profiles to assess the risk of a lending loan to the customer. Following a set of parameters have been considered while calculating and analyzing the credit risk:

- **Age Information** : This parameter reveals the current age of the borrower

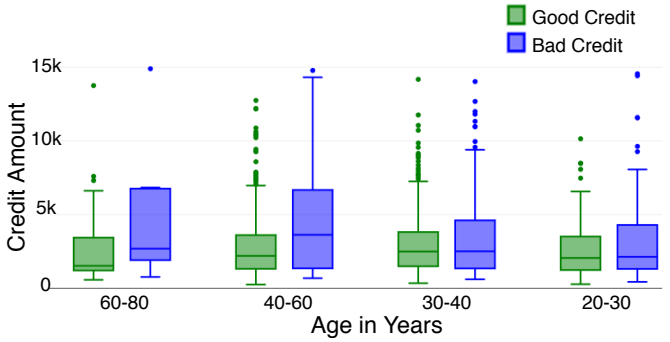

Fig. 4: Age wise distribution for credit risk

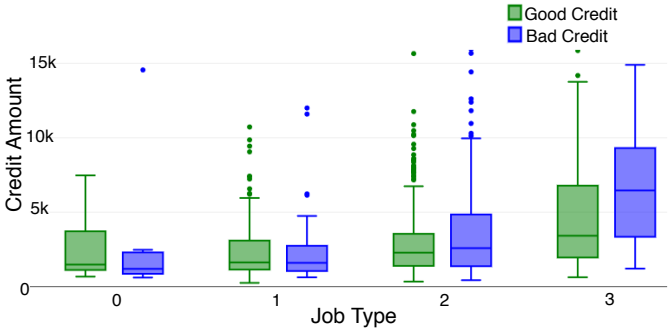

Fig. 5: Job wise distribution for credit risk

- **Sex** : This parameter reveals the sex of the borrower
- **Job Profile**: Job parameter is divided into four categories, i.e., unskilled & nonresident, unskilled & resident, skilled, and highly skilled. The unskilled nonresident category is marked as job type 0, unskilled & resident is marked as 1, skilled is marked as two, and highly skilled is marked as 3 in Fig. 5.
- **Housing Type** : Housing can be either own, rented or free
- **Saving Account Balance**: It shows the average balance of savings account. We can use 4 categories of saving account type as little, quite rich, moderate and rich.
- **Credit Amount Pending**: This parameter shows the loan amount taken in the history
- **Credit Duration**: This shows the duration of the credit amounts taken in the past
- **Credit Purpose**: This parameter reveals the purpose of the credit taken

In this section, we plot the variation of credit score based on the above parameters using the UCI data set [48]. Lenders do not trust all borrowers equally. We depict how lending an amount is a function of the category of borrowers. Good credit or Good risk are cases in which lenders received repayment from borrowers. On the other hand, in cases where the repayment was failed is depicted using bad risk or bad credit.

Fig. 4 shows the distribution of credit risk involved with respect to the age group of the borrowers. Each box plot is divided into four quartiles. The box refers to the middle two quartiles. The line below the box is the first quartile, and

the line above the box is the fourth quartile. The dark line between the boxes refers to the median of the range. We can see from the distribution that in the case of age group 60-80, the median of the box for good credit is too low. This depicts that a maximum number of people in the age group do timely repayment only when the credit amount is low.

Fig. 5 shows a similar distribution with respect to the job type pf the individuals. We can observe from the box plots that the investors feel more confident in lending higher amounts to the highly skilled people as compared to the unskilled and nonresident individuals. So the parameters for credit score calculation are not always the same for all classes of people. The amount of credit risk varies with the creditworthiness of the people involved. The next section discusses how optimal investment (ξ) varies with different lenders and borrowers.

V. Credit Score Interpretation of Investors

When there is no trusted third party, credit scoring requires proper interpretation depending on the kind of lenders. For example, lending of $500\$$ can be seen differently by a different set of lenders. The risk and return is a function of a particular lender and its inherent characteristic. We make a model for three kinds of investors, opportunistic, neutral, and risk-averse. The system model is presented in Fig. 2

We take a simple use case to highlight the need of prospect theory. For example a investor has an option of getting \$900 or take a 90% chance of winning \$1000 (and a 10% chance of winning 0)? Most investors avoid the risk and take the \$900, although the expected outcome is the same in both cases. However, if an investor is asked to choose between losing \$900 and take a 90% chance of losing \$1000, most of the investors would probably prefer the second option (with the 90% chance of losing \$1000) and would thus engage in the risk-seeking behavior in the hope to avoid the loss.

For the behavior modeling of investors, we construct the objective function. The key elements of investors or lenders are discussed here:

1) Lenders decide a reference point of neutrality. Based on this reference point, the investments are differentiated into losses or gains.
2) Different behaviors are displayed by the lenders concerning the losses or gains. The value function is convex for the losses and concaves for the gains.
3) The sensitivity of the lenders is higher in case of losses as compared to the gains.
4) Small probabilities are associated with excessive weights, whereas the large probabilities are ignored based on a weight function. The weight function is a nonlinear transformation of the objective probability.

In this section, we present model the optimal allocation of lenders based on behavioral economics using prospect theory. The theory was presented by two psychologists Daniel Kahneman and Amos Tversky, and in the late 20th century, they called it prospect theory because it was a theory of how people form decisions about prospects and a prospect is a gamble it's about people's decisions under uncertainty using [8] and [49]. lenders have two options, one consists of one risk-free asset (no lending), with 0 return, and another possibility of lending (risky asset) with a stochastic return of ψ. Let W_0 denote the investors initial wealth. An amount of ξ is invested in the risky asset and the remaining wealth, $W_0 - \xi$, is not invested. Then the individuals wealth at the end is given by:

$$W = W_0 + \xi\psi. \tag{1}$$

Let the excess return on the risky asset over the risk-free rate as $\tilde{\gamma} = \psi$.

$\tilde{\gamma}$ can take both positive values and negative values with positive probabilities. The deviation from the reference level where the reference level being the initial wealth satisfies:

$$D(\xi) = W - W_0 = \xi\tilde{\gamma}. \tag{2}$$

The prospect theory model incorporates a value function that represents how lenders value things. For every investor τ is utility gain for investor or return parameter, while χ is the risk or loss parameter, λ captures loss aversion. The utility for given ψ as the credit score is given by:

$$U_\psi = \begin{cases} \psi^\tau, & \psi \geq 0 \\ -\lambda(-\psi)^\chi, & \psi < 0. \end{cases}$$

In financial mathematics, there's a weighting function that shows how people infer or how they deal with uncertainty or risk. It is also referred as distortion risk measure w. w is related to the cumulative distribution function of the return on investment. w^g and w^l denote the weight function for gains and losses respectively as shown in following equation.

$$w = \begin{cases} w^g, & \mathrm{k} > 0 \\ w^l, & \mathrm{k} < 0, \end{cases}$$

$$w^g(\psi) = \frac{\psi^\gamma}{(\psi^\gamma + (1-\psi)^\gamma)^\gamma},$$

$$w^l(\psi) = \frac{\psi^\delta}{(\psi^\delta + (1-\psi)^\delta)^\delta},$$

γ = 0.61 and δ = 0.69 are experimental evaluated constants. Since the functions w^g are increasing, positively homogeneous, invertible and twice differentiable. where

$$w = \begin{cases} \mathrm{w}^g\ (0) = w^l\ (0) = 0 \\ \mathrm{w}^g\ (1) = w^l(1) = 1. \end{cases}$$

Using prospect theory, the objective function of the lender (V) for any D is given by:

$$V(D) = \int_0^{+\infty} w^g(D)dU^+(D) - \xi^\chi \int_{-\infty}^{0} w^l(D)dU^-(D). \tag{3}$$

From equation 2, we get $\tilde{\gamma} = \frac{D}{\xi}$, then

$$dD = \xi(d\tilde{\gamma})dU^{+}(D) = \tau D^{\tau-1}dD,$$

$$dU^{+}(D) = \tau(\xi(\tilde{\gamma}))^{\tau-1}\xi(d\tilde{\gamma}),$$

$$dU^{-}(D) = \lambda\chi D^{\chi-1}dD,$$

$$dU^{-}(D) = \lambda\chi(\xi(\tilde{\gamma}))^{\chi-1}\xi(d\tilde{\gamma}),$$

$$w^{g}(\tilde{\gamma}) = \tau(w^{g}(D))(\tilde{\gamma})^{\tau-1},$$

$$w^{l}(\tilde{\gamma}) = \lambda\chi(w^{l}(D))(\tilde{\gamma})^{\chi-1}.$$

$$V(D) = \xi^{\tau}\int_{0}^{+\infty} w^{g}(\tilde{\gamma})d\tilde{\gamma}^{+} - \xi^{\chi}\int_{-\infty}^{0} w^{l}(\tilde{\gamma})d\tilde{\gamma}^{-}. \quad (4)$$

The objective function (**P**) for every lender is defined as:

$$\mathbf{P}: \max_{\xi\geq 0}((G(\tilde{\gamma}))\xi^{\tau} - L(\tilde{\gamma})\xi^{\chi})). \quad (5)$$

where

$$\begin{cases} G(\tilde{\gamma}) = \int_{0}^{+\infty} w^{g}(\tilde{\gamma})d\tilde{\gamma}^{+} \\ L(\tilde{\gamma}) = \int_{0}^{+\infty} w^{l}(\tilde{\gamma})d\tilde{\gamma}^{-}. \end{cases}$$

$$\Omega(\tilde{\gamma}) = \frac{\int_{0}^{+\infty} w^{g}((\tilde{\gamma}))d\tilde{\gamma}}{\int_{0}^{+\infty} w^{l}((\tilde{\gamma}))d\tilde{\gamma}}.$$

We define another parameter $\Omega(\tilde{\gamma})$ as a performance measure, which assesses the quality of the risky asset. The optimal holding in the risky asset depends on the $\Omega(\tilde{\gamma})$. This ratio quantifies the upside potential of the risky asset (measured by $G(\tilde{\gamma})$ relative to its downside potential (measured by $L(\tilde{\gamma})$).

Lemma 1. *The objective function **P** is concave in ρ when*

$$\tau < \chi \quad \& \quad 0 \leq \Omega(\tilde{\gamma}) \leq 1.$$

To prove this we show that $\nabla^{2}\mathbf{P}(\xi) < 0$. This can be shown as follows. We consider the value of our objective function as

$$\mathbf{P}(\xi) = ((G(\tilde{\gamma}))\xi^{\tau} - L(\tilde{\gamma})\xi^{\chi})).$$

The first and second order derivatives of the objective function with respect to ξ are given by

$$\nabla\mathbf{P}(\xi) = \frac{d(G(\tilde{\gamma})\xi^{\tau})}{d\xi} - \frac{d(L(\tilde{\gamma})\xi^{\chi})}{d\xi},$$

$$\nabla^{2}\mathbf{P}(\xi) = \frac{d^{2}(G(\tilde{\gamma})\xi^{\tau})}{d\xi^{2}} - \frac{d^{2}(L(\tilde{\gamma})\xi^{\chi})}{d\xi^{2}}$$

$$= \tau^{2}(G(\tilde{\gamma})\xi^{(\tau-2)} - \chi^{2}(L(\tilde{\gamma})\xi^{(\chi-2)}) \leq 0.$$

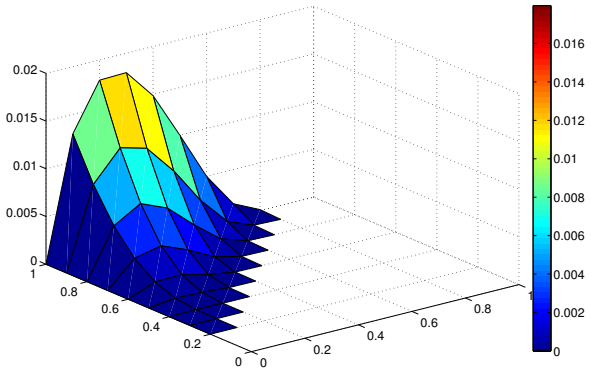

Fig. 6: variation of ξ with respect to τ and χ for Ω = 0.2

Note that the term $\nabla^{2}\mathbf{P}(\xi)$ above is always negative as $\chi > \tau$ & as $\Omega(\tilde{\gamma} \leq 1$, so $G(\tilde{\gamma}) \leq L(\tilde{\gamma})$. This proves that the objective function $\mathbf{P}(\xi)$ is concave with respect to ξ.

Lemma 2. *A unique optimal allocation $\xi_{O} \in \xi$ exists which maximises $(G(\tilde{\gamma})\xi^{\tau} - L(\tilde{\gamma})\xi^{\chi})$ and is given by*

$$\xi_{O} = \left(\frac{\tau}{\chi}\right)^{\frac{1}{\chi-\tau}}\Omega(\tilde{\gamma})^{\frac{1}{\chi-\tau}}.$$

This follows from the fact that the objective function $\mathbf{P}(\xi)$ is a concave function of ξ (as shown in Lemma 1). Since the objective function **P** is concave in ξ when $\tau < \chi$ & $0 \leq \Omega(\tilde{\gamma}) \leq 1$, then optimal allocation ξ_{O} is given by:

$$\nabla\mathbf{P}(\xi) = \frac{d(G(\tilde{\gamma})\xi^{\tau})}{d\xi} - \frac{d(L(\tilde{\gamma})\xi^{\chi})}{d\xi} = 0,$$

$$\xi_{O} = \left(\frac{\tau}{\chi}\right)^{\frac{1}{\chi-\tau}}\Omega(\tilde{\gamma})^{\frac{1}{\chi-\tau}}. \quad (6)$$

VI. Results & Discussion

This is a unique work in this field as to the best of our knowledge. Thus, there do not exist any related works to compare our results. Since blockchain is secure distributed ledger, and all data being stored on ledge. The time evaluation for credit score evaluation is nominal resulting fa larger number of transactions per second. The immutability of leader also provides resistance to malicious activities currently present in lending systems.

However, we present the variation of an optimal investment. For every investor, τ is a utility gain, while χ is the risk or loss parameter. The parameter Ω is the performance measure that assesses risk & return on investment in the borrower. Ω is the ratio of return vs. risk and is considered fixed for a borrower. ξ is an optimal investment $(0-1)$ that an investor is likely to invest in. 0 means no investment, and 1 means complete investment. Prospect theory shows that people generally tend to avoid risk even at the cost of less return. The loss parameter is greater than utility gain ($\chi > \tau$). We model optimal investment for three borrowers having different return

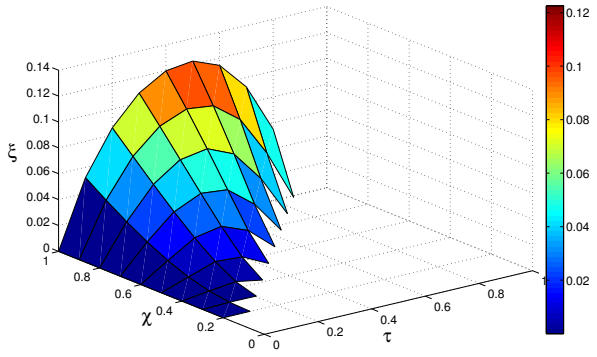

Fig. 7: variation of ξ with respect to τ and χ for $\Omega = 0.7$

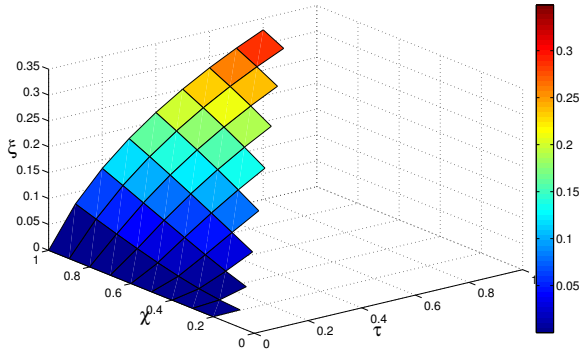

Fig. 8: variation of ξ with respect to τ and χ for $\Omega = 1$

vs risk (Ω = 0.2, Ω = 0.7, Ω = 1.0). χ & τ vary from 0 to 1. From Eq. 6 we have,

$$\xi = \left(\frac{\tau}{\chi}\right)^{\frac{1}{\chi-\tau}} \Omega^{\frac{1}{\chi-\tau}}.$$

TABLE I: Variation in ξ for different τ at χ=0.8

$\chi = 0.8$	$\xi(\tau$=0.1)	$\xi(\tau$=0.4)	$\xi(\tau$=0.7)
Ω = 0.2	0.004	0.0005	0.0036
Ω = 0.7	0.018	0.03	0.05
Ω = 1.0	0.04	0.072	0.1

Fig. 6, 7, 8 shows variation of ξ with respect to τ and χ for Ω = 0.2, Ω = 0.7 & Ω = 1 respectively. As the Ω increases, so there are more chances of return for a given risk, and hence investment increases. For example, for $\Omega = 0.2$ (Fig. 6), when χ = 0.9 & τ = 0.5, the optimal investment (ξ) = 0.0041. ξ increases to 0.094 when $\Omega = 0.7$ (Fig. 8) and reaches value of 0.23 for $\Omega = 1$ (Fig. 9) for same χ & τ.

TABLE II: Variation in ξ for different χ at τ=0.3

$\tau = 0.3$	$\xi(\chi$=0.5)	$\xi(\chi$=0.8)	$\xi(\chi$=1.0)
Ω = 0.2	0.00001	0.005	0.018
Ω = 0.7	0.016	0.06	0.1
Ω = 1.0	0.05	0.12	0.18

For an investor, initially, as utility gain (τ) increases, the investment (ξ) increases. Lenders want more profit, so increasing τ increases ξ. But utility gain saturates, and further increasing the investment would increase the risk of loss. Ω factor dominates in deciding the optimal investment as utility gain is further increased. When Ω= 0.2, return vs risk is low (Fig 7). Hence ξ increases till τ = 0.3 and then decreases. On the other hand, when return vs. risk is high (Fig. 9), the optimal investment increases with an increasing value of τ (ref. Table I). Another observation is that as the loss risk-taking potential (χ) of lenders increases, so is the optimal investment (ξ) for a given τ. Lenders would be investing more, as shown in Table II.

VII. Numerical Analysis

We performed a simulation analysis using Amazon Mechanical Turk (MTurk) data provided by Cam Davidson [50]. MTurk is a crowdsourcing website for businesses (known as Requesters) to hire remotely located "crowdworkers" to perform discrete on-demand tasks that computers are currently unable to do. It is operated under Amazon Web Services, and is owned by Amazon. The simulation analysis was performed using Python on Macbook Air, Mojave OS with 8GB Ram and 128Gb SSD.

Consider two investment scenarios:

- Investment A: Investor has X% chance of getting a return on Investment A (Higher Payoff)
- Investment B: Investor has Y% chance of getting a return on Investment B (Lower Payoff)

We simulate for different values of X & Y and evaluate the probability of choosing option A with the change in the risk on return. If everyone was rational, and hence indifferent to the two choices, the probabilities should hover around 0.5. This is clearly not the case. The simulation heat map is presented in figure 9. As expected, people are loss averse: every point in the lower-diagonal is where Investment A had a high probability of success than B. The matrix shows that most points in here are greater than 50%, thus people chose the safer bet more often. The exception to the above point is the fact that 1% is chosen more favourably over 2%. This is an instance of the possibility effect. People are indifferent between 1% and 2%, as they are both so rare, thus will pick the one with larger payoff.

VIII. Comparison of Utility vs Prospect Theory

This is a unique work in this field as to the best of our knowledge. Thus, there do not exist any related works to compare our results. However, in Fig. 10 we provide a comparison between the prospect theory and Utility theory based ideology using blockchain presented in [51] and [52]. The expected utility theory deals with the analysis of situations where individuals must make a decision without knowing the outcomes. Unlike expected utility theory, prospect theory predicts that preferences will depend on how a problem is framed. If the reference point is defined such that an outcome is viewed as a gain, then the resulting value function will be concave and decision makers will tend to be risk averse.

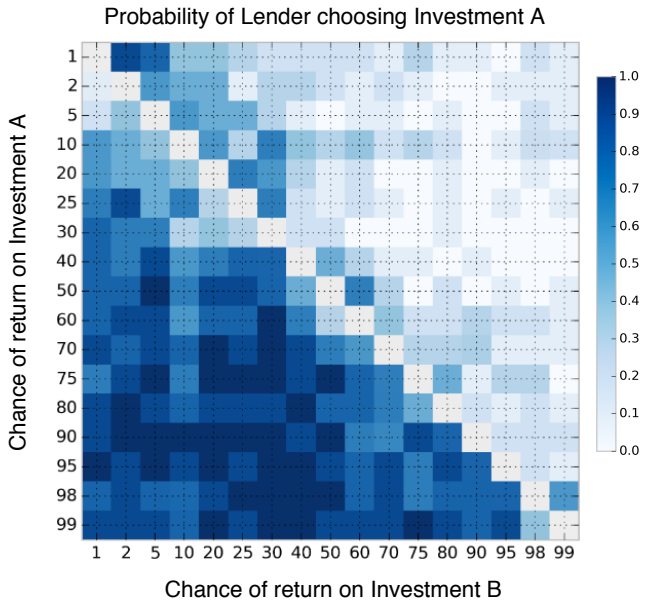

Fig. 9: Probability of Choosing Investment A over B

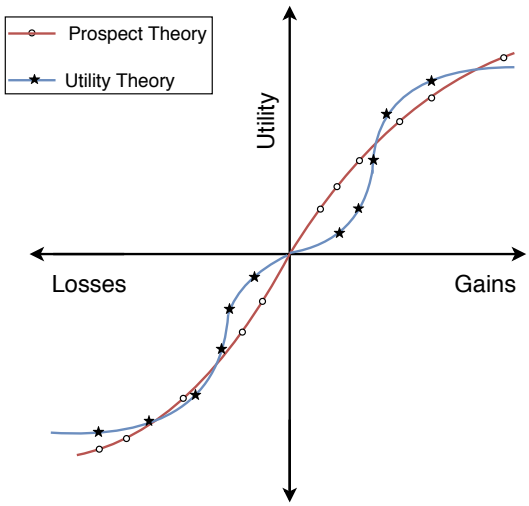

Fig. 10: Comparison of utility theory and prospect theory in terms of utility.

The prospect theory says that investors value gains and losses differently, placing more weight on perceived gains versus perceived losses. An investor presented with a choice, both equal, will choose the one presented in terms of potential gains.

IX. Conclusion

Credit scoring is used to evaluate the creditworthiness of an individual. It is a statistical parameter that quantifies the risk of lending money to a borrower. This paper presents a secure and decentralized model to calculate the credit score of an individual that eliminates the need of trusted parties and transaction history aggregation. The credit score calculated in this model considers both financial as well as non financial information of an individual to calculate the creditworthiness. This paper uses the prospect theory to model the optimal investment strategy for different risk vs. return scenarios. The results show that the probability of lending is different for different types of lenders, depending upon the level of gain or risk acceptable to the lenders.

References

[1] World Bank, "Credit Reporting," http://www.worldbank.org/en/topic/financialsector/brief/credit-reporting, online; accessed 29 January 2019.

[2] X. Wang, D. Jeong, R. Chang, and W. Ribarsky, "Riskva: A visual analytics system for consumer credit risk analysis," *Tsinghua Science and Technology*, vol. 17, no. 4, pp. 440–451, Aug 2012.

[3] J. M. Redondo and F. Ortin, "A saas framework for credit risk analysis services," *IEEE Latin America Transactions*, vol. 15, no. 3, pp. 474–481, March 2017.

[4] FICO, "Credit Education," https://www.myfico.com/credit-education, online; accessed 19 December 2018.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, 2019.

[6] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[7] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[8] C. Gong, C. Xu, M. Ando, and X. Xi, "A new method of portfolio optimization under cumulative prospect theory," *Tsinghua Science and Technology*, vol. 23, no. 1, pp. 75–86, 2018.

[9] Y. L. Eddy and E. M. N. E. A. Bakar, "Credit scoring models: Techniques and issues," *Journal of Advanced Research in Business and Management Studies 7, Issue 2*, pp. 29–41, 2017.

[10] A. F. Atiya, "Bankruptcy prediction for credit risk using neural networks: A survey and new results," *IEEE Transactions on Neural Networks*, vol. 12, no. 4, pp. 929–935, July 2001.

[11] P. J. G. Lisboa, T. A. Etchells, I. H. Jarman, C. T. C. Arsene, M. S. H. Aung, A. Eleuteri, A. F. G. Taktak, F. Ambrogi, P. Boracchi, and E. Biganzoli, "Partial logistic artificial neural network for competing risks regularized with automatic relevance determination," *IEEE Transactions on Neural Networks*, vol. 20, no. 9, pp. 1403–1416, Sep. 2009.

[12] W. Lin, Y. Hu, and C. Tsai, "Machine learning in financial crisis prediction: A survey," *IEEE Trans. on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42.4, 2012.

[13] W. Luo, H. Jiang, and D. Zhao, "Rating credits of online merchants using negative ranks," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 5, pp. 354–365, Oct 2017.

[14] R. S. Gaonkar and N. Viswanadham, "Analytical framework for the management of risk in supply chains," *IEEE Transactions on Automation Science and Engineering*, vol. 4, no. 2, pp. 265–273, April 2007.

[15] D. D. Wu, D. L. Olson, and C. Luo, "A decision support approach for accounts receivable risk management," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 12, pp. 1624–1632, Dec 2014.

[16] K. K. Lai, "A new fuzzy support vector machine to evaluate credit risk," *IEEE Trans. on Fuzzy Systems*, vol. 13, no. 6, pp. 820–831, Dec 2005.

[17] C. Wang, D. Han, Q. Liu, and S. Luo, "A deep learning approach for credit scoring of peer-to-peer lending using attention mechanism lstm," *IEEE Access*, vol. 7, pp. 2161–2168, 2019.

[18] D. Roman and G. Stefano, "Towards a reference architecture for trusted data marketplaces: The credit scoring perspective," in *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016, pp. 95–101.

[19] J. Lohokare, R. Dani, and S. Sontakke, "Automated data collection for credit score calculation based on financial transactions and social media," in *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*. IEEE, 2017, pp. 134–138.

[20] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[21] R. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 29–37, sep 2018.

[22] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, July 2018.

[23] Colendi, "Blockchain-Based Credit Scoring Outshines The Big Three," https://medium.com/colendi/, online; accessed 01 January 2019.

[24] J. Daimani, "Meet Bloom, The Company Transforming Credit Scores With Blockchain," https://www.forbes.com/sites/jessedamiani/2017/11/14/meet-bloom-the-company-transforming-credit-scores-with-blockchain/, online; accessed 09 Feburary 2019.

[25] M. Ersin Tekmen, "Combating Global Poverty on Blockchain," https://blog.colendi.com/, online; accessed 14 January 2019.

[26] E. J. Elton and M. J. Gruber, "Modern portfolio theory, 1950 to date," *Journal of Banking & Finance*, vol. 21, no. 11-12, pp. 1743–1759, 1997.

[27] J. Quiggin, *Generalized expected utility theory: The rank-dependent model*. Springer Science & Business Media, 2012.

[28] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of Risk and uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.

[29] Y. Wang, W. Saad, A. I. Sarwat, and C. S. Hong, "Reactive power compensation game under prospect-theoretic framing effects," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4181–4193, 2018.

[30] I. Levi, "The paradoxes of allais and ellsberg," *Economics & Philosophy*, vol. 2, no. 1, pp. 23–53, 1986.

[31] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1310–1322, 2017.

[32] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2543–2585, thirdquarter 2018.

[33] N. Kumar, M. Kumar, and R. Patel, "Capacity and interference aware link scheduling with channel assignment in wireless mesh networks," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 30–38, 2011.

[34] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[35] N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "A multi-tenant cloud-based dc nano grid for self-sustained smart buildings in smart cities," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 14–21, 2017.

[36] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, July 2018.

[37] N. Kumar, N. Chilamkurti, and S. C. Misra, "Bayesian coalition game for the internet of things: an ambient intelligence-based evaluation," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 48–55, 2015.

[38] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149, pp. 51–61, 2020.

[39] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, 2020.

[40] V. Hassija, V. Chamola, G. Han, J. Rodrigues, and M. Guizani, "Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology*, 2020.

[41] Z. Yang, W. Lang, and Y. Tan, "Fair micropayment system based on hash chains," *Tsinghua Science and Technology*, vol. 10, no. 3, pp. 328–333, June 2005.

[42] V. Hassija, M. Zaid, G. Singh, A. Srivastava, and V. Saxena, "Cryptober: A blockchain-based secure and cost-optimal car rental platform," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*. IEEE, 2019, pp. 1–6.

[43] V. Hassija, V. Chamola, N. G. K. Dara, and M. Guizani, "A distributed framework for energy trading between uavs and charging stations," *IEEE Transactions on Vehicular Technology*, 2020.

[44] M. O'Neill and M. J. B. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags," *IET Computers Digital Techniques*, vol. 4, no. 1, pp. 14–26, January 2010.

[45] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Transactions on Services Computing*, pp. 1–1, 2018.

[46] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[47] V. Hassija, V. Saxena, V. Chamola, and R. Yu, "A parking slot allocation framework based on virtual voting and adaptive pricing algorithm," *IEEE Transactions on Vehicular Technology*, 2020.

[48] Kaggle, "German Credit Risk," https://www.kaggle.com/uciml/german-credit, online; accessed 01 March 2019.

[49] C. Bernard and M. Ghossoub, "Static portfolio choice under cumulative prospect theory," *Mathematics and financial economics*, vol. 2, no. 4, pp. 277–306, 2010.

[50] CamDavidsonPilon, "Homegrown analysis of prospect theory: Math, turkers and python," https://github.com/CamDavidsonPilon/decision-weights, online; accessed January 2020.

[51] C. Catalini, R. Jagadeesan, and S. D. Kominers, "Market design for a blockchain-based financial system," *Available at SSRN 3396834*, 2019.

[52] M. Swan *et al.*, "Blockchain theory of programmable risk: black swan smart contracts," *Blockchain Economics: Implications Of Distributed Ledgers-Markets, Communications Networks, And Algorithmic Reality*, vol. 1, p. 171, 2019.

X. Author Biography

Vikas Hassija received the B.Tech. degree from Maharshi Dayanand University, Rohtak, India, in 2010, and the M.S. degree in telecommunications and software engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2014. He is currently pursuing the Ph.D. degree in IoT security and blockchain with the Jaypee Institute of Information and Technology (JIIT), Noida, where he is currently an Assistant Professor. His research interests include the IoT security, network security, blockchain, and distributed computing.

Gaurang Bansal received the B.E. M.E. degree in Computer Science from Birla Institute of Technology and Science, Pilani, India, in 2018 and 2020 respectively. He has authored more than 10 publications in top tier confences and Journals like IEEE INFOCOM, IEEE Globecom, IEEE ICC, IEEE Transaction on Vehicular Technology etc. His research interests include the IoT security, network security and distributed computing.

Vinay Chamola received the B.E. degree in electrical and electronics engineering and masters degree in communication engineering from the Birla Institute of Technology and Science, Pilani, India, in 2010 and 2013, respectively, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016. He is currently an Assistant Professor in BITS-Pilani, Pilani Campus. His research interests include Green communications and networking, 5G network management, Internet of Things and Blockchain.

Neeraj Kumar (M'16-SM'17) received the Ph.D. degree in computer science engineering from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is currently a Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored or co-authored more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, etc.

Mohsen Guizani (S'85-M'89-SM'99-F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor at the Computer Science and Engineering Department in Qatar University, Qatar. He is an IEEE Fellow and currently serves as the Editor-in-Chief of the IEEE Network Magazine and editor in several international journals.