Blockchain Driven Three Domain Secure 2.x in Digital Payment Services Architecture

Vikas S. Shah(✉)

Knights of Columbus, New Haven, CT 06510, USA
shah_vikas_s@usa.net

Abstract. Due to the recent advancements in digital commerce, consumers expect real-time digital payment convenient and available across channels as more connected devices become payment devices. It offers consumers to pay in-store or online purchases in many diversified ways. The three domains secure protocol evolved to version 2.x (3DS2) supporting the development in digital payment domain and its rapid adaptation. The specification includes the provisioning of the application-based purchases enabling risk-based decisions to authenticate the consumer transactions. 3DS2 enhances consumers' checkout experiences through out-of-band authentication. It eliminates the need for enrollment process and static password supporting non-payment activities and native mobile. The primary challenges to implement 3DS2 are dimensioning the risks, real-time variability in the risk factors, and precision to compute the accumulative risk associated with the individuals. Financial services, merchants, and consumers are enabled to connect into the blockchain network using application programming interfaces (APIs). It alleviates participants of Blockchain network from having to build out their own distributed transactions' server nodes. This paper proposes a blockchain-driven 3DS2 service architecture framework that integrates the risk-based decisions and provides a secure communication platform in digital commerce. We illustrate the increased level of authenticity, maintainability, extendibility, and flexibility in the digital payment ecosystem with the industry case study of membership-based in-store or online charitable contribution campaigns during point-of-sale.

Keywords: Application programming interface (API) · Blockchain (BC) · Digital activity (DA) · Frictionless flow · Risk factor (RF) · Three domain secure 2.x (3DS2)

1 Introduction

In 2019, the online fraudulent transactions increased to 27% and 42% consumers experienced the unauthorized payment activities [1]. The results impacted entire supply-chain, including delays in shipments, consumer traffic, and in-store purchases. Survey of 166 United States' merchant conducted by Federal Reserve Bank of Minneapolis indicates that the Card Not Present (CNP) is the top payment threat to retailers [2]. The Nilson Report announced the losses from worldwide fraud on credit cards, debit cards and prepaid cards hit $27.85 billion last year on a total card sales volume of $40.582 trillion [3].

J. E. Ferreira et al. (Eds.): SERVICES 2020, LNCS 12411, pp. 11–27, 2020.
https://doi.org/10.1007/978-3-030-59595-1_2

The Merchants pay up to 3.5% in the transaction fees. Besides, merchants are subject to flat fees for point-of-sale terminal usage, network charges, and incidental expenses such as chargebacks in case of fraud or disputes. Every dollar of fraud now costs banks and credit unions about $2.92, a 9.3% increase over 2017. The payment industry has seen enough data breaches to affect at least a few billion people across the globe.

The merchants, retailers, consumers, and issuers are always in the exploration of approaches to reduce payments fraud in the digital business ecosystem effectively. According to statistics presented in [4], the average active connections per day across the globe exceeded 8.3 billon. The connected ecosystem and increasing reach of Internet-of-Thing (IoT) enabled devices to facilitate consumer to pay from diversified geographic locations and currencies. Half of the digital business transactions declined due to suspected fraud.

Three domain server protocol prevents fraudulent activities in card-based payment transactions through multiple channels and devices. It is widely adapted and utilized to secure the payment. The specification of advancement in 3DS2 is already formulated and available by Europay, MasterCard, Visa Contactless (EMVCo) [5]. Many organizations have already started offering the 3DS2 services and capabilities to the connected ecosystems of payment. 3DS2 uses token-based and biometric authentication. It uses risk-based decisions for authentication using additional data during the transactions. The consumer checkout experience is anticipated to be seamless and secures irrespective of the devices, applications, and methods payment. The challenge for 3DS2 is the accuracy in identifying the risk factors and computing the risks in real-time. Due to the increased number of options introduced for real-time payment transactions, the evolution in risk factors, assessment, and corresponding computations are imminent.

Blockchain can modernize a payment and capture the evolving risks in real-time. It offers tokenization and authenticity of transactions between multiple parties with minimal operational and technical frictions [6]. However, Blockchain protocols and governance are immature to content the compliances associated with the eCommerce payments. Its ability to support the challenging non-functional requirements of payment services has yet to be proven [7]. We identified the Blockchain driven 3DS2 Service Fabric Architecture framework (BC2SF) formulation 3DS2 Application Programming Interfaces (APIs). The APIs can be classified and governed based on evolving characteristics of payment ecosystems. Additionally, the BC2SF supports the new way of digital payments introduced in the future by means of evolving digital technologies and payment industry including digital currencies.

The core component of the BC2SF is 3D Secure 2.0 Service Fabric (3DS2SF). The 3DS2 specification emphasizes on the real-time evaluation of modeling and analyzing the risk factors associated with the payment transactions. The BC provides detail history of the transaction in context of the digital payment to identify the risk factors and their relationships with the ongoing transaction(s). The risks factors can have multiple or nested levels of dimensions. The examples of the dimensions for risk factors includes geolocation, devices, applications, currency (or amount), internet connectivity paradigms, and products (or services). For instance, if the payment has been initiated from the unauthorized or unrecognized device over the previous transactions pertaining to the related BC transactions of the specific person or eCommerce website then it requires computing

risk on the specific digital payment transaction to identify the amount can be allowed for purchasing.

We investigated issues and challenges of digital payment due to advancements in digitalization of business and introduction of 3DS2 in existing payment ecosystem in Sect. 2. Section 3 outlines the requirements of 3DS2 and indictive coordination alongside Blockchain technology. Section 4 presents the BC2SF framework components and their responsibilities. It provides methodology to specify and evaluate risk factors to identify real-time authentication decision for payment ecosystem. Section 5 illustrates the empirical use case of charitable contribution during point-of-sale (PoS) using BC2SF. Eventually, Sect. 6 concludes our findings and future direction to advance the risk governance.

2 Challenges of Digital Payment Methods and 3DS2

Three Domain Secure (3DS) specification is primarily composed of acquirer domain, interoperability domain, and issuer domain, as indicated in Fig. 1. Acquirer establishes a relationship with a merchant to accept payment card transactions [8]. The acquirer domain has a requester client, server environment, integrator, and payment authorization mechanisms. The client can either be application-based or browser-based. The server collects necessary data elements for 3DS messages [5]. It authenticates, validates, and ensures the messages between the requester of the payment and cardholders.

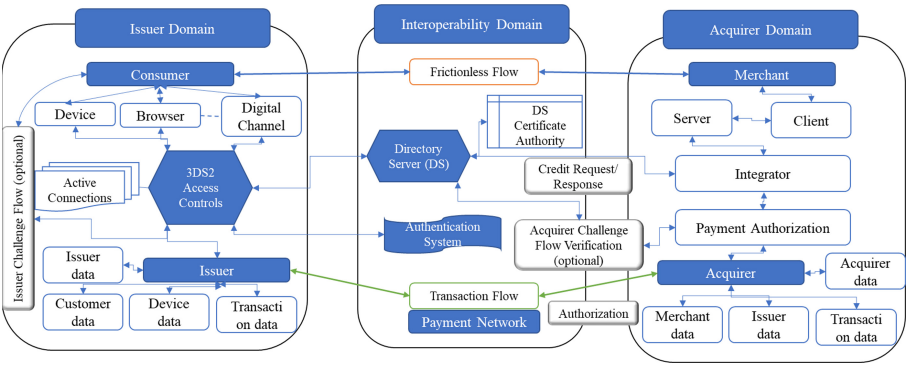

Fig. 1. Communication between three domains of 3DS2 specification.

The integrator provides the functional interface between the 3DS requestor environment and the 3D secure messages between client and server. The interoperability domain consists of Directory Server (DS), Directory Server Certificate Authority (DSCA), and Authorization System. The issuer domain manifests cardholder, consumer device, issuer information, and access control server (ACS).

3DS2 defines three types of client and server flows for the checkout process during any purchase irrespective of the digital payment channel or method, that is, frictionless flow, challenge flow, and transaction flow. Frictionless flow is new to 3DS2. Challenge

flow and traditional transaction flow are associated and updated with frictionless flow requirements [8]. Frictionless flow [9] introduces risk-based authentication to determine whether the cardholder is required to perform challenge flow for further authentication. The risk-based authentication primarily dependents upon two factors, that is, the additional data captured during the checkout process of purchases and transaction history of the customer performing the payment. The data can be of multiple types, including cardholder purchasing behavioral pattern data, device information, and merchant authorization detail. Merchants are required to capture an extensive data set from the customer during the checkout process. The transaction flow retrieves the browser and mobile devices' data.

During our analysis of various approaches to implement 3DS2, we identified complexities and extendibility challenges of implying novel 3DS2 between client, acquirer, and interoperability domains. Following are the list of identified issues for 3DS2 to be effective.

Risk Factors: The risk factors vary for different types of businesses, geolocation, and personal profile of the individual. The 3DS2 needs to include dynamic of defining and configuring the risk factors depending on the different dimensions in consideration [10] and [11]. For instance, a customer with an international travel history and travel incentive account has a higher risk of currency level fraud and mishaps over online purchasing activities.

Payment Methodologies: The Internet-of-Thing (IoT) enabled devices advancing to capture new types of data to increase security and safeguard the identity of the individual. Client domains require to extend capabilities that can accept additional types of payment methods as well as authentication mechanisms. The MasterPass offering by the Master Card Corp. is a classic example of the new payment types [12]. Additionally, every bank and providers started offering the number of different ways to pay online as well as in-store purchases.

Customer Data: If the bank doesn't have enough information, then it can request a challenge step-up flow to authenticate the transaction and prompt the customer to provide additional data during 3DS2 The dependency on the quality of the data of the customers are very high. If the customer data are not consistent and up to date, then probabilities of the customers receiving the correct level of challenge question are lower [13]. The acquirers receive customer information from the card-issuing bank, public network, and government records during the card application. The data to verify the customer are typically old or not valid during the step-up flow to authenticate the transaction. Customer may have lived in the county for 3 to 4 weeks and may not have remembered it. Contrarily, an old acquittance, can take advantage of this information.

Payment Gateway Types: Generally, merchants facilitating eCommerce technologies utilize the payment gateway. The payment gateway providers implement the different encryption mechanisms as well as approval workflow for the transactions [14]. Any change or upgrade to the payment gateway requires either new interfaces or modification to the existing interfaces. Besides, the testing of the new or updated payment gateway with 3DS2 requires extensive testing before offering to the customers. Many types of

payment gateways are available, including pro-hosted payment gateway and direct payment gateway. Pro-hosted payment gateway relies on the user data provided from the web or mobile application, whereas direct payment gateway periodically inquires the payment completion. Both the methods are for different purposes, and various types of messages flow between the merchant and payment gateway.

Merchant: 3DS2 emphasized on the authenticating the customers to avoid the fraudulent transaction. It has very little to no attention provided for malicious merchants and the validity of the merchant-specific device applications to accept the payment [15]. 3DS2 leverages the concept of the trusted merchant within the merchant account or the corresponding mobile applications. However, it is susceptible to exfiltrate. If the customer unknowingly configure browser to add trusted sites (as an add-on), then the third-party application during browsing can add the trusted merchant to the browser.

3 Synergy of 3DS2 Requirements and Blockchain Technologies

Internally, the 3DS2 server collects the necessary data elements from any or all the components to initiate the authentication. It has three types of information collected to analyze, that is, device information, browser information, and merchant risk information [5]. If a merchant has a mobile application with integration domain component of 3DS2, then it needs to capture the necessary information directly from the device to process the transaction. The device information consists of 12 data elements [16]. However, iOS-specific information has 13 elements, whereas Android-specific information has 36 elements. It includes the type of platform and the specific Internet Protocol (IP) address associated along with device name, device model, device's operating system information, time zone, location, and screen resolution. If transactions are conducted on the merchant's website through a browser, data is captured by the 3DS server. The browser information includes the content type, IP address, Java enablement flag, screen resolution, language, time zone, and user agent [5] information. The merchant is also required to collect additional cardholder information to help improve the accuracy of the risk-based authentication. The merchant risk information consists of account, purchase, prior transaction authentication, and account authentication information.

The merchant shares this information with the card issuer for analyses and identification of the risk level based on the specifics of the transaction. It allows the issuer to make an informed decision as to whether additional authentication step-up flow is required. The 3DS2 specification indicates computing the risk. If the risk is below a certain threshold, then the issuer will approve the cardholder authentication. For this specification to handle the transaction, it must generate Payment Tokens (PTs) for risk-based authentication. The PTs ranges are shared and configured on the DS. PTs routed to the DS and consequently to the ACS. During the transaction, the authentication request needs to detokenize PTs. The PT Indicator in the request message provides the risk associated with the transaction.

In [17], an extensive fraud processing method provides a merchant to implement discounting, acceptance, and fraud rules based on the card type. It emphasizes on the risk with the card types over the risk levels associated with the consumers and the patterns of

transactions. On the other hand, the method identified in [18] focuses on authentication system. It computes the decision based on device data during a checkout process of a current transaction on a merchant website and contextual data of the customer. The risk scoring mechanism for payment card transaction presented in [19] is based at least in part on the transaction data and infrastructure data associated with the transaction. It defines the acceptable risk to the merchant against the pre-defined risk threshold. Data mining techniques including decision tree, logistic regression, random forest and neural network were constructed with the cleaned dataset to detect risks of credit card defaulters in [20]. It predicts risk associated with merchants with credit card defaulters with 82% accuracy. The comparative analysis is presented in [21] with multiple machine learning (ML) classification on the highly imbalanced datasets consisting of credit card transactions. It indicates that any additional datasets linked with consumers to be considered to identify risks and changing the threshold require merchants to undertake a hefty level of assumptions in their risk classification. The existing approaches are incompetent to evolve the merchant's payment ecosystem in a way to insert or update the risk levels as well as new paradigms to compute the risks at runtime during transaction processing.

A blockchain consists of a peer-to-peer (P2P) communication overlay network. Each network node connects to other nodes through defined protocol and discovery processes [22]. The research presented in [23] takes advantage of the delay-tolerant nature of blockchains to deliver banking services to remote communities. The blockchain users can handle regular transaction processing with the use of a base station feature capabilities offering connectivity within the local area. The bank only joins in processing currency exchange requests. In [24], the conceptual architecture for a blockchain-based Personal Data and Identity Management System (BPDIMS) is illustrated using trust protocol and off-chain repository.

The decentralized and distributed linked list built with hash pointers [25] is available to all participants involved in the payment transactions in Blockchain-based payment authentication. [26] establishes a new architecture called secure pub-sub (SPS) without middleware, that is, blockchain-based fair payment with reputation. In SPS, publishers publish a topic on the blockchain, and subscribers specify a message by depositing to the topic. The [27] prescribes Blockchain digital certificate methodology to avoid fraudulent transactions. It generates a digital certificate for the transaction data by blockchain-enabled electronic ownership token. It allows transferring the electronic ownership of the token.

The blockchain-enabled ecosystem can provide the following advantages and resolves challenges of 3DS2 specification to be implemented for the payment networks.

- Blockchain protocol consistently connects and communicate customers, merchant, acquirer, issuers, and payment, gateway providers. It can provision role-based transaction information in the nodes.
- The block maintains the chain of transactions and associated risks for a specific customer (or set of customers). It achieves the prior transaction authentication requirements of 3DS2 without real-time computation as a recent transaction block already carries the authentication information with it.

- Blockchain allows customization of tokens in consideration of many dimensions and risk factors including device, browser, and merchant information specified by 3DS2. It can validate merchant and cardholders (customers) in the specification of the token.
- The blocks can be extended as well as interoperable with the new transactional and IoT device information. It can also include these factors for risk computation and authentication.

The blockchain configuration includes consensus in the perception of validator nodes for the issuer to validate blocks with the transactions [28]. Consequently, different types of consensus can be implied depending on the type of participant in the transaction, that is, public, private, and permissioned (or consortium) blockchain. Typically, 3DS2 is a candidate of consortium blockchain where participants are pre-selected, and the issuer has the authorization to modify the participant list.

4 Blockchain Driven 3DS2 Service Fabric Architecture Framework

To address and resolve the challenges of managing complexities of PTs of 3DS2 in the conditions of computing risks in real-time, we have identified the Blockchain driven 3DS2 Service Fabric Architecture (BC2SF). It correlates, computes, and advances risks associated with the specific transaction under the influence of changing characteristics of risks factors through Blockchain-enabled services or Application Programming Interfaces (APIs). The blockchain nodes include a trace or period trace of the transaction history beginning at the activation of the cards to the most recent payment in terms of blocks. It inherits detail of the transactions for each consumer, including device, browser, and merchant risk information required by 3DS2 specification. The transactions in the blocks are not limited to a specific card; it has the link to the potential payments associated with the consumers whether it is performed utilizing any device, card, or other means of payment. The services under the Blockchain network provision shared repositories and common processes in the nodes to compute the risks based on the risk factors in the context of the transaction. It entails an efficient and accurate specification of risks associated with payments.

Figure 2 provides components of the BC2SF incorporating friction fewer payment options and real-time risk computing capabilities. The primary components of the BC2SF framework are 3DS2 service fabric (3DS2Sf), Blockchain API Manager (BCAPIm), Authentication Decision Manager (ADm), Blockchain Node Manager (BNm), Acquirer Configurator (Acon), and Digital Channel Director (DCd). 3DS2Sf is formulated with Risk Factor Association Manager (RFAm), Risk Rater (RRt), Risk Orchestrator (ROr), and Risk Feedback Engine (RFe).

3DS2 Service Fabric (3DS2Sf): The primary responsibility of the 3DS2Sf is to provide the platform to integrate the acquirer domain, interoperability domain, and issuer domain through the services (or APIs). The 3DS2Sf invokes the frictionless flow of the 3DS2 specification through service. It evaluates the risks associated with the transactions based on the risk factors and risk rating techniques utilized for the specific classification of the service for the type of transaction chain maintained within the Blockchain network nodes. It is accountable to decide whether the transaction needs one more level of further

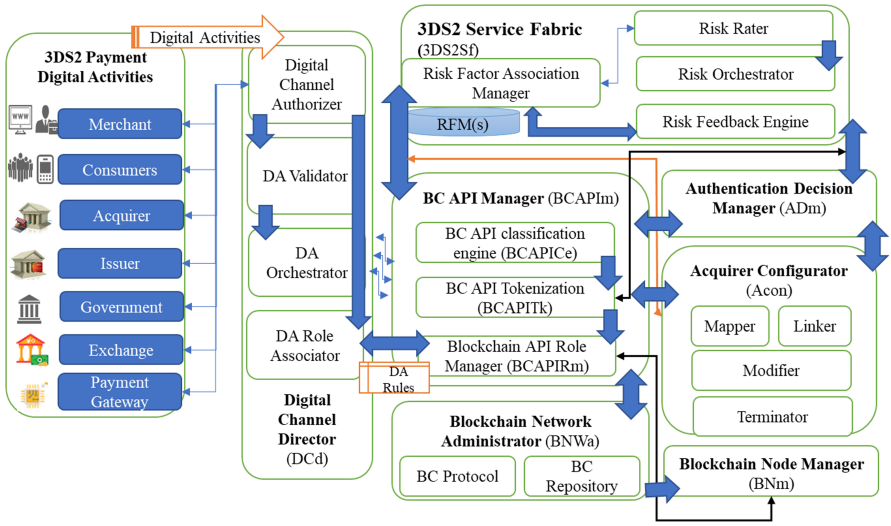

Fig. 2. Blockchain driven 3DS2 service fabric architecture framework (BC2SF).

authentication. 3DS2Sf connects with the ADm with analyzed information within the services for further action towards the payment transaction in context.

Risk Factor Association Manager (RFAm): RFAm defines RFA (Risk Factor Association) model (RFM) to identify, place, and compute risk factors associated with the specific transaction or set of transactions in real-time. RFM consists of risks factors for the device, browsers, and merchant risk authentication. It can also consist of subcategories of risk factors for each of the data elements associated with the device, browser, and merchant risk authentication during the payment. Figure 3 represents the elements of the RFM. RFM provides the contract and agreement between the issuers, merchants, acquirers, and cardholders in adherence to avoid fraudulent digital activities during frictionless flow for payment. In Fig. 3, RIC represents the risk computations, "n" presents the number of participants' digital activities, and "r" characterizes number of risks for the particular digital activity in context.

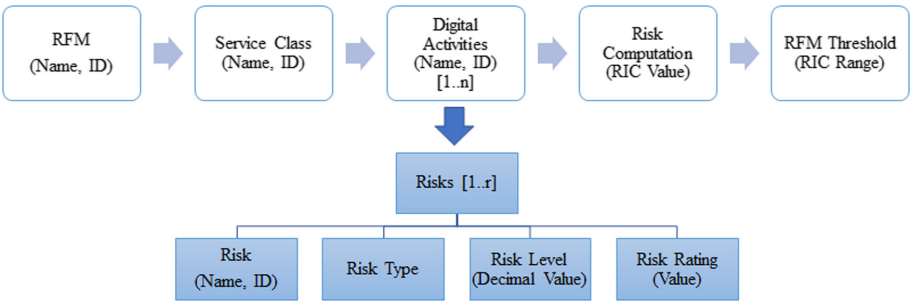

Fig. 3. Risk factor association model (RFM) elements.

Risk Rater (RRt): RRt is to define the type of risk and its rating when it occurs during the transaction flow within the 3DS2 ecosystem. The risk rating scheme can be changed in real-time through RRt component of the RFAm. The real-time change in the RRt scheme (or technique) will be implied either to the specific types or set of transactions in the proximity of the RFA model.

Risk Orchestrator (ROr): ROr provides the hierarchy of the risks across the RFM. The ROr specifies the order of risks from high to low. The RFM can either define, adapt, or dynamically change risk orchestration using ROr. The ROr dilutes the rating of the specific risk in real-time by the delta specified within the RFM depending on the position of the risk in the orchestration.

Risk Feedback Engine (RFe): RFe is the sanity check whether the computed risks are within the range of specific threshold. It specifies and adjusts the risk threshold for RFA model. If the transaction is supposed to be unauthorized, however, it is computed to be authorized, then it decreases the threshold for future transactions of the same type corresponding to the associated risk factors.

Authentication Decision Manager (ADm): ADm is the final decision provided whether the frictionless flow must go through additional authorization, denied, or approved. It validates the computation performed using RFAm and the risk threshold from the RFe to provide the decision for each transaction. The runtime validation of risk threshold for a specific type of transaction can only be performed using ADm. ADm interacts with BCAPIm and BNm to initiate either challenge flow or transaction flow required to proceed with the purchase or transaction. ADm is also the final authority to decide on challenge flow upon receiving additional information of the cardholder. It identifies the cardholder and authorized to proceed with the transaction or disapprove the transaction. It again informs BCAPIm to initiate transaction flow.

Blockchain API Manager (BCAPIm): BCAPIm is responsible for classification, management, and error handling of services. Each RFM is mapped to the service (or API) to compute the risks associated with the payment transaction(s). The challenge flow and transaction flow are also associated with the specific APIs within the BCAPIm. If the ADm doesn't approve the frictionless flow and it needs to initiate the challenge flow API, then BCAPIm initiates the challenge flow to receive more information from the cardholder. It connects with ADm to take further action against the information received. If the transaction flow is initiated by ADm, then BCAPIm's transaction flow APIs performs the transaction and registers it to the block associated with the Blockchain node through BNm.

BC API classification engine (BCAPICe), Blockchain API Role Manager (BCAPIRm), and BC API Tokenization (BCAPITk) are the essential components of the BCAPIm. BCAPICe specifies the classification of the services interacting with BC nodes and frictionless payment. Acquirer associated with the merchant (or set of merchants) can define the classification scheme. It can be based on the type of transaction, geolocation diversity, type of merchants, type of devices, mobile applications, type of consumers, and other customarily defined class. The acquirer can select to place classification with multiple dimensions.

BCAPITk connects BCAPICe and 3DS2Sf to recognize RFM for the specific classification through ADm. It identifies the RFM to be implied for the specific transaction based on the classification specified by the acquirer. It provides access and visibility of the transaction chains associated with the specific transaction with the token and its accessibility for the merchant and issuing bank. The ADm executes the specified RFM and computes the risks in real-time. The BCAPITk generates the token and associate computed risk to it.

BCAPIRm provides the accessibility of the token to various participants of the transaction. The transaction may involve multiple issuers, merchants, brokers, cardholders, and acquirers. Each participant can have a specific role. BCAPIRm manages the role hierarchy and rules associated with the roles during the transaction. BCAPIRm also defines the validator role responsible for validating the Blockchain nodes.

Blockchain Node Manager (BNm): The transfer of information between Blockchain and BCAPIm in the framework occurs using a cryptographic protocol that arrives at a consensus among participant nodes to update the blocks. BNm defines the consensus mechanism based on the Blockchain topologies selected within the payment ecosystem, that is, private, public, or permissioned (or consortium) blockchain. The BNm in association with the BCAPIRm manages the accessibility of the Blockchain nodes and their blocks. It also performs validation of the nodes recognizing validator assigned by the BCAPIRm.

Blockchain Network Administrator (BNWa): The BNWa provides administrative aspects of Blockchain to connect acquirers, merchants, issuers, and consumers in the vicinity of the transactions through the Blockchain nodes. Multiple blockchain protocols can be utilized to achieve consensus among participant nodes for updating the blockchain ledger. Each such protocol will have to be evaluated in the context of the participants of payment and transaction, the use case, and requirements of an enterprise. If the payment gateway is utilized intermediator, then it can either introduce or leverage one or more protocols to recognize and validate the transaction. BNWa provides capabilities to establish the protocol and streamline communication between the BCAPIm and blocks of shared repository carrying the history associated with the specific transaction in context.

Acquirer Configurator (Acon): The Acon is responsible for administering each service under the scope of specific acquirer or type of acquirer. It is composed of four different elements of service administration, that is, Mapper, Linker, Modifier, and Terminator. It interfaces with BCAPIm and 3DS2Sf to map the services (or APIs) the frictionless, challenge, and transaction flows. The Acon linker establishes links between the RFM and APIs. The Acon modifier updates the mapping and linking at runtime. It also maintains the versions of the updated mapping and linking. Acon terminator is accountable for successfully dismiss the invalid and unauthorized transactions as recommended by the ADm. The terminated transaction is also recorded to the blockchain node through BCAPIm.

Digital Channel Director (DCd): The DCd provides the means to connect diversified users with the BC2SF framework. The customer, issuer, merchant, and acquirer can

utilize many ways to perform various activities during the checkout process of the purchases, as indicated in the responsibilities of each component. DCd is responsible for validating and orchestrating these activities. It is also the first line of defense against faulty payment activities and transactions. It consists of Digital Channel Authorizer (DCa), Digital Activity Validator (DAv), Digital Activity Orchestrator (DAo), and Digital Channel Role Associator (DCr). DCa authorizes new or existing digital channel for the payment. DAv validates the activities and Dao orchestrator the digital activities in alignment with the checkout process, including receiving payment information and biometrics of the cardholder. DCr associate the role of the specific digital activity with the BCAPIRm to recognize the rules to be implied for the specific digital activity.

The digital activities, the roles associated with digital activities, and actions differ significantly across the checkout process. It is eminent during in-store purchases as well. For example, the cardholder decides to pay with the mobile payment application for the groceries as well as the eye examination performed in the supermarket, facilitating both the capabilities. Multiple merchants, banks, and insurance company participate during the transaction. The risk factors with the transaction need to be analyzed at runtime as multiple types of payments are included in the transaction. The RFAm associates the risk factors, the orchestration of risks, and individual risk rating in the unified RFM as API. The risk can be computed for the entire transaction (in Block Ia). The ADm registers the transaction to block as authorized transaction upon approval. The Blockchain has capabilities to link the transaction through blocks for merchants as well as cardholders. For instance, if the cardholder has a secondary card issued to the family member, then ADm immediately links and compute the risks corresponding to the inflight transaction (in Block Ib) by the secondary card. If one of the identified risk factors is the payment limit with the threshold of the $250, then ADm ensures the accumulative payment for both transactions (Block Ia and Block Ib). If the amount exceeds the $250 threshold, then it rejects the later transaction (Block Ib). However, the rejected transaction (Block Ib) still been recorded for future reference to compute the risk for the subsequent transaction (in Block II).

BC2SF enables to build an industry-agnostic payment ecosystem to complete the implementation of 3DS2 specification within the dilemma increasing number of digital channels for payment. It prohibits fraudulent digital activities and provides early indicators equally to the cardholder and merchants. It brings role-based transparency and accuracy between acquirers and issuers. 3DS2Sf and ADm recognizes and ensures the existing, new, and updated risks of digital activities during the checkout process and payment transactions. The BC2SF also resolves interoperability challenges and transparency between participants of the payment ecosystem to recognize the risks with the transactions.

5 In-store and Online Charitable Contribution Use Case of BC2SF

Charitable Giving Report indicates that the most common approach preferred by the consumers for charitable donation over two years was checkout donations during point-of-sale (PoS) purchases [26]. 2018 survey reveals that 79 charitable contribution campaign initiatives brought in $486.37 million [24]. Charitable contribution campaigns are

crucial for not-for-profit or nonprofits to achieve the target for noble causes. Individual giving makes up nearly 70% of donations around the globe [29]. According to the National Center for Charitable Statistics, 1.56 million tax-exempt organizations exist in the United States [30]. The organizations must enable digital channels in compelling ways to donate and contribute to charity events. Blackbaud's 2017 Charitable Giving Report indicates that the most common approach preferred by the consumers for charitable donation over two years was checkout donations during point-of-sale (PoS) purchases [31]. 2018 survey reveals that 79 charitable contribution campaign initiatives brought in $486.37 million [29].

As retailers increase their digital presence and work to offer 3DS2 frictionless payment options to their consumers, they are also bringing nonprofit counterparts along with the point-of-sale systems [29]. It raises a need for a system that allows the consumer to donate to charitable trust or organization based on having observed them [32]. It is useful for the consumer to be able to restrict how the recipient spent donation through selecting charitable trust or a specific campaign. It is mandatory to secure delivery of the donation to the recipient to prevent fraudulent recipients. A merchant's PoS terminals and online checkouts can prompt micro-donations for local and national nonprofits and adding a donation to a specific charity campaign. The BC2SF can seamlessly handle the scenario and dynamically update the list of nonprofits, not-for-profit, or charitable contribution campaigns as a workflow. We identified 15 metalevel activities requires to be performed during the checkout of purchases to accommodate charitable contribution. Table 1 represents the RFM associated with service classification "Member Donation". The RFM provides the example risk rating (RR), risk level (RL), DA Threshold (DAT), and RFM threshold (T) to define the relationship between the merchant, consumer, and charitable trust. T provides the acceptable range to approve the transaction for purchases and donation.

All the branches of the merchant or set of merchants associated with acquirer utilizing BC2SF can have consistent RFM across their value-chain. The RFM can also have diversification based on various dimensions in the Blockchain network. For instance, if the RFM focused on the United States, then the service class needs to be "United State Member Donation" through BCAPICe. Although each merchant can generate its way to compute the overall risk associated with RFM and risk rating scheme for the RFM, we created risk computation (RIC) based on Eq. 1.

$$\mathrm{RIC} = \left(\sum_{i=1}^{n} (RLiXRRi)\right) \Big/ \mathrm{n} \tag{1}$$

"n" presents the total number of DA for the specific service classification. The RR represents the risk rating between 1 to 5 where DA with risk rating 1 is at the lowest risk and 5 is at the highest risk provided by the RRt. The RL specifies the risk level in the orchestration of the risk retrieved from the ROr. The RIC considers the averaging the product of risk level and risk rating associated with each digital activity. The formula indicates the precedence of the risks associated with the lower-level digital activities in the hierarchy is 10% higher than the previous level of digital activities. For example, DA# 1, DA# 2, and DA# 5 are at the risk level 1 and RL is 1 for them in Table 1. DA# 3 (underneath DA# 2) and DA# 6 (underneath DA# 5) are at risk level 2 and RL is 1.1 for them. DA# 13 and DA# 14 are at nested level of DA# 12 as the digital activities

Table 1. Digital activities of member donation service.

RFM: POS charitable contribution
Service classification: member donation

DA#	DA	Role	Risk	RL	RR	DAT
1	Enter purchase amount	Merchant	Items or number of purchased items	Level 1a	1	
2	Enter card number	Consumer	Customer privacy	Level 1b	5	≪4-digit range≫
3	Enter donation amount (with purchase)	Consumer	In appropriate donation amount	Level 1b.1	2	10% (of purchases)
4	Select & validate charitable trust	Consumer	Classification & rating of charitable trust	Level 1b.2	3	
5	Receive & validate card holder	Acquirer	Invalid person or transaction	Level 1c	2	
6	Verify purchase and donation amount based on card transactions	Payment gateway (or acquirer)	In appropriate amount or exceeding threshold value	Level 1c.1	2	$250
7	Approve & notify card holder	Acquirer	No activities & invalid transaction history	Level 1c.2	4	
8	Challenge questions (if required)	Acquirer	Invalid challenge questions & answers	Level 1c.3	3	≪Pre-authorized questions≫
9	Pay & deduct amount from card holder for purchase	Issuer	Card holder credentials & amount	Level 1d	2	
10	Receive amount for purchases	Merchant	Account not available for deposit	Level 1d.1	2	

(*continued*)

Table 1. (*continued*)

RFM: POS charitable contribution **Service classification**: member donation						
DA#	DA	Role	Risk	RL	RR	DAT
11	Pay & deduct amount for donation	Issuer	Card holder credentials & amount	Level 1e	3	
12	Receive donation amount	Charitable trust	Account not available for deposit	Level 1e.1	2	
13	Tax deduction & exemption	Charitable trust	Mismatching of Tax codes & amount	Level 1e.11	2	≪Tax codes for charity≫
14	Tax authorization & notification	Charitable trust	Unauthorized category of donation	Level 1e.12	3	≪Donation categories≫
15	Tax computation & credits	Government	Unregistered tax information & codes	Level 1f	2	≪Tax exempt organizations≫
RIC = 2.78. **T** (for transaction to be approved) = [0 to 3]						

are performed by the charitable trust in association to the government irrespective of the consumer or type of consumer. It is the reason, the RL is 1.11 for DA# 13 and 1.12 for DA# 14 indicating the risk is only 1% incrementally higher over the primary digital activity, that is, DA# 12.

The BC enables token to carry the RFM with its RIC. BCAPITk manages all the issued tokens across BC network. The value of the token is consistent between all the participants, including merchant, acquirer, issuer, charitable trust, and government. The ADm decides based on the runtime value of the RIC against the threshold defined for RFM to approve the transaction. ADm can facilitate the transaction for purchases, however, rejecting the donation amount through the Acon modifier using the API dedicated to the charitable contribution campaign event defined in BCAPIm. The BNm ensures to register the transaction irrespective of the approved or rejected by ADm. It is utilized by acquirer during the subsequent transaction by the consumer at the same or different merchant to identify RR for the DA, as indicated in Table 1. DA# 7. Based on the status of the transaction, the RFe provides feedback to RFAm and adjust the RR for the specific risk associated with DA through RRt component.

The BC2SF heavily relies on APIs to process and validate transactions as well as to insert the risk levels and thresholds. BCAPIm is responsible to discover APIs in correlation to transaction and risk in real-time. The BCAPIm quality-of-service (QoS) across the payment ecosystem improves the discovery of the APIs at runtime as indicated in [33]. The challenge for the acquirer is to select the appropriate QoS model based on the learnings of the number of transactions of a specific pattern and the type of

consumers. The acquirer will not have visibility of all the transactions performed by the specific type of consumers as consumers utilize diversified payment methods issued by different banks. The acquirer needs to adapt QoS prediction model [34] to improve the prediction accuracy between the APIs to compute and insert risk levels at runtime. 3DS2Sf's API consumptions require to be based on the recognized combination of historic and predicated transaction patterns.

The advancements in 3DS2 require many organizations to include different scenarios and diversification in the payment transactions during purchases. In [35], the extensible PoS device is identified to register a third-party application for changing transaction on the PoS device for merchants. It provides a user interface during a purchase using one of a registered application module and a payment module. [36] claims that the charity collection processes are not transparent and charitable organizations struggle to gain donors' trust and interest. The proposed blockchain-based charity management platform provides a seamless, secure, auditable, and efficient system. It enables charity collection process using crypto wallets, Initial Coin Offering (ICO), economic model, and introduces CharityCoin (CC) as a digital currency.

6 Conclusion

In this paper, we presented the blockchain services-based framework to implement 3DS2. The primary differentiation to implement 3DS2 is the runtime risk computing for the transaction during the payment. The BC2SF architecture framework provides APIs to capture and utilize device data, browser (or mobile application) data, merchant risk data to compute risks and embed the RIC with tokens in real-time for each transaction. Blockchain enables the granular level of risks accuracy based on the DA and associated roles. It decreases the complexity and difficulty of analyzing transaction history during the purchases and correlate them with the risk of the new transaction. The tokenization and RIC scheme of BC2SF introduces risk computation capabilities for all the participants in the transaction, including the consumers, merchant, acquirers, and issuers. BCAPIm implements core functions of frictionless payment and challenge flow specified in3DS2 standards. It is extensible to update and generate service classifications based on the dimensions and in advancements of digital channels. BC2SF DCd seamlessly integrates upcoming methods of payments to facilitate consumers and merchants, including digital wallet capabilities.

BC2SF promotes configurable solution for the payment methods with real-time decisions on authentication and non-payment user authentication. It dynamically extends services to meet specific regulatory requirements, including proprietary out-of-band authentication solutions by card issuers. The benefits are visible for 3DS2 risk-based authentication, tokenization, and evolving paradigms for risk assessment during frictionless payment utilizing BC2SF. The primary research interest is to advance BC2SF governance processes considering different types of business transactions and automation among participants of the payment ecosystem.

References

1. Guta, M.: 27% of Online Sales End Up Being Fraudulent Transactions, Small Business Trends, December 2019
2. Federal Reserve Bank of Minneapolis: Fighting Fraud in the e-Commerce Channel: A Merchant Study, June 2018
3. The Nilson Report, Card Fraud Losses Reach $27.85 Billion, November 2019
4. Liu, S.: Internet of Things - Statistics & Facts, Statista, March 2020
5. EMVCo, LLC: EMV 3-D Secure Protocol and Core Functions Specification v2.2.0, December 2018
6. Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., Zheng, D.: Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. Telecommun. **74**(7–8), 401–411(2019)
7. Hasan, H.R., Salah, K.: Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access **6**, 65439–65448 (2018)
8. Corella, F., Lewison, K.P.: Frictionless web payments with cryptographic cardholder authentication. In: Stephanidis, C. (ed.) HCII 2019. LNCS, vol. 11786, pp. 468–483. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30033-3_36
9. Corella, F., Lewison, K.P., Pomian and Corella LLC: Scheme for frictionless cardholder authentication. U.S. Patent Application 16/533,771 (2020)
10. Ab Hamid, N.R., Cheng, A.Y.: A risk perception analysis on the use of electronic payment systems by young adult. order **6**(8.4), 6–7 (2020)
11. Ali, M.A., van Moorsel, A.: Designed to be broken: a reverse engineering study of the 3D secure 2.0 payment protocol. In: Goldberg, I., Moore, T. (eds.) FC 2019. LNCS, vol. 11598, pp. 201–221. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32101-7_13
12. Shrilatha, S., Priya, M.M.L.: The role of customers to attain sustainable development of cashless transaction by shifting to mobile wallets at Vellore city. Stud. Indian Place Names **40**(18), 11–29 (2020)
13. Ma, S., Fildes, R.: Forecasting third-party mobile payments with implications for customer flow prediction. Int. J. Forecast. **36**(3), 739–760 (2020)
14. Dhobe, S.D., Tighare, K.K., Dake, S.S.: A review on prevention of fraud in electronic payment gateway using secret code. Int. J. Res. Eng. Sci. Manag. **3**(1), 602–606 (2020)
15. Corella, F., Lewison, K.: Fundamental Security Flaws in the 3-D Secure 2 Cardholder Authentication Specification (2019)
16. EMVCo, LLC: EMV 3-D Secure SDK—Device Information Data Version 1.4, October 2019
17. Weber, L.: Account type detection for fraud risk, Visa International Service Association, United States patent application US 16/367,935 (2019)
18. Tomasofsky, C.P., et al.: Systems and methods for providing risk based decisioning service to a merchant, Mastercard International Inc., United States patent US 10,614,452 (2020)
19. Roche, M.F., Salaman, K.: Decision making on-line transactions, US Bancorp, National Association, United States patent application US 16/164,609 (2020)
20. Leong, O.J., Jayabalan, M.: A comparative study on credit card default risk predictive model. J. Comput. Theor. Nanosci. **16**(8), 3591–3595 (2019)
21. Parthasarathy, G., et al.: Comparative Case Study of Machine Learning Classification Techniques Using Imbalanced Credit Card Fraud Datasets, SSRN 3351584 (2019)
22. Xia, Q., Sifah, E.B., Huang, K., Chen, R., Du, X., Gao, J.: Secure payment routing protocol for economic systems based on blockchain. In: 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 177–181. IEEE, March 2018
23. Hu, Y., et al.: A delay-tolerant payment scheme based on the ethereum blockchain. IEEE Access **7**, 33159–33172 (2019)

24. Faber, B., Michelet, G.C., Weidmann, N., Mukkamala, R.R., Vatrapu, R.: BPDIMS: a blockchain-based personal data and identity management system. In: Proceedings of the 52nd Hawaii International Conference on System Sciences, January 2019
25. Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R.S.: Blockchain in payment card systems. SMU Data Sci. Rev. **1**(1), 3 (2018)
26. Zhao, Y., Li, Y., Mu, Q., Yang, B., Yu, Y.: Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems. IEEE Access **6**, 12295–12303 (2018)
27. Allen, C.M., Hale, C., Nomura, C.: Systems and Methods that Utilize Blockchain Digital Certificates for Data Transactions, Kountable Inc., U.S. Patent Application 15/787,674 (2018)
28. Zouina, M., Outtai, B.: Towards a distributed token-based payment system using blockchain technology. In: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1–10. IEEE, April 2019
29. Hessekiel, D.: Charity Checkout Remains Strong, Even In A Changing Retail Landscape, Leadership Strategy, Forbes Media LLC (2020)
30. McKeever, B.: The Nonprofit Sector in Brief 2018, National Center for Charitable Statistics, December 2018
31. Blackbaud Institute: 2018 Charitable Giving Report: How Fundraising Performed in 2018, February 2019
32. Bax, N.G.: Identifying Recipients for Restricted Giving. U.S. Patent Application 16/045,681 (2020)
33. Sha, J., Du, Y., Qi, L.: A user requirement-oriented web service discovery approach based on logic and threshold petri net. IEEE/CAA J. Automatica Sinica **6**(6), 1528–1542 (2019)
34. Luo, X., et al.: Generating highly accurate predictions for missing QoS data via aggregating nonnegative latent factor models. IEEE Trans. Neural Netw. Learn. Syst. **27**(3), 524–537 (2015)
35. Beatty, J.D., El Calamawy, T.M., Abrams, J.W., Quinlan, M.J., Blattman, J.: Extensible point-of-sale platforms and associated methods, Clover Network Inc., U.S. Patent 10,580,029 (2020)
36. Farooq, M.S., Khan, M., Abid, A.: A framework to make charity collection transparent and auditable using blockchain technology. Comput. Electr. Eng. **83**, 106588 (2020)