SMU Data Science Review

Volume 1 | Number 1 Article 3

2018

Blockchain in Payment Card Systems

Darlene Godfrey-Welch
Southern Methodist University, dgodfreywelch@smu.edu

Remy Lagrois
Southern Methodist University, rlagrois@smu.edu

Jared Law
Southern Methodist University, jlaw@smu.edu

Russell Scott Anderwald
Southern Methodist University, randerwald@smu.edu

Daniel W. Engels
Southern Methodist University, dwe@smu.edu

Recommended Citation

Godfrey-Welch, Darlene; Lagrois, Remy; Law, Jared; Anderwald, Russell Scott; and Engels, Daniel W. (2018) "Blockchain in Payment Card Systems," *SMU Data Science Review*: Vol. 1 : No. 1 , Article 3.
Available at: https://scholar.smu.edu/datasciencereview/vol1/iss1/3

Blockchain in Payment Card Systems

Scott Anderwald, Darlene Godfrey-Welch,
Remy Lagrois, Jared Law, Daniel W. Engels

Southern Methodist University, Dallas, Texas 75205
{randerwald, dgodfreywelch, rlagrois, jlaw, dwe}@smu.edu

Abstract. Payment cards (e.g., credit and debit cards) are the most frequent form of payment in use today. A payment card transaction entails many verification information exchanges between the cardholder, merchant, issuing bank, a merchant bank, and third-party payment card processors. Today, a record of the payment transaction often records to multiple ledgers. Merchant's incur fees for both accepting and processing payment cards. The payment card industry is in dire need of technology which removes the need for third-party verification and records transaction details to a single tamper-resistant digital ledger. The private blockchain is that technology. Private blockchain provides a linked list built with hash pointers used to record encrypted transactions in a structured manner. It is a decentralized and distributed and available to all participants involved in the transaction. Private blockchain removes the need for third-party validators, thereby reducing fees and increasing the Merchant's overall transaction value.

Keywords: private blockchain, sensitive information, cryptographic hash, cryptography, payment card, transaction.

1 Introduction

Use of the internet[1] by individuals has grown exponentially from 1990 to 2016. By 2016, 76% of the United States and 46% of the World's individuals were using the internet [1]. The growth of [2] the internet has spawned an increase in personal convenience applications. These applications extend to multiple industries (education, banking, healthcare) where a "person" or personal interaction is the focal point of the experience. The end-to-end interaction between a person and an application culminates in a digital transaction where every action is captured and recorded in a ledger or tracking log.

Digital transactions account the majority type of commodity exchanges performed today. Critical elements of a digital transaction include participants, personal information of the individual participating in the transaction, an asset, the exchange or transaction, and the technology used to record the transaction, such as a ledger.

A participant provides various pieces of information be required to participate in a digital transaction using an electronic system. These often include, but are not limited

[1] Glossary Entry; See Graphical Comparison in Appendix B, Fig. 18.

to legal name, physical address, mailing address, social security number, bank number(s), user login names, user passwords, and so on. This information is qualified as sensitive, in that the disclosure of this information may result in a loss of advantage to the owner. Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual [3].

The level of sensitivity varies by the type of information. In decision theory, the expected value of perfect information (EVPI) is the price that one would be willing to pay to gain access to perfect information [4]. Unfortunately, today, the value of sensitive information is also a factor of the cost associated with protecting the information from unwanted disclosure [5]. Information is an asset.

A digital transaction, in this discussion, is defined as a seamless and non-traditional system involving one or more participants, where transactions take place without the need for currency. Thus, the transaction as a "cashless" or non-currency based digital payment. Extending the concept of digital transactions to payment, the exchange of a commodity for digital payment consists of

- a transaction initiation (consumer),
- use of a digital instrument issued by a financial institution (issuing bank) such as a payment card, mobile pay, eWallet,
- authorization-of-use by the issuer (card network, payment processor),
- acceptance by a merchant financial institution (acquiring bank),
- verification of funds to back the worth of the exchange (acquiring bank)
- lastly, a final confirmation of the purchase (merchant).

Today, transactions most often require the disclosure of sensitive information to conduct the authorization and validation subtransactions to verify the involved parties, confirm the funds or legalities, and register the transaction. Because most of these transactions are electronic, each activity is quickly captured, and written to a ledger, along with relevant sensitive information[2].

A ledger records all business activity as a transaction. Every market or network defines a ledger. Ledgers record asset transfers between participants. A transaction ledger records the transaction from the point of initiation through confirmation of award of the commodity. Sensitive information is recorded or traceable to the transaction in its entirety. This can include identification of the commodity exchanged, security credentials, worth of the transaction, legalities, personal identification relevant to the authorization step, and financial information relevant to the authorization step. The transaction ledger contains sensitive information that can be traced directly back to an individual or entity. This traceability is multi-directional—or available to all parties participating in the transaction. The issue with multi-directional traceability is potential exposure of sensitive information about participants and the transaction.

There are many informational exchange points in payment card processing between financial institutions and third-party validators. These points of exchange include various types of information--name, address, social security number, bank numbers, payment card numbers. Compounding the issues is the use of multiple ledgers where every entity involved in a transaction, records its version of the transaction. Bits and

[2] Glossary entry; See Appendix B Examples of Sensitive Information.

pieces of sensitive information distribute to multiple sources who are operating their set of unique set of security practices.

Payment card processing requires computing, network, storage resources as well as oversight and management. Resources and management incur costs—costs associated with both consuming and supplying payment card services. The cost of a transaction is the responsibility of those involved in the transaction. These costs are often passed on to the merchant, and eventually the consumer, in the form of fees paid to the payment card issuing bank and card network.

A centralized virtual ledger instrument that can control participant access, encrypt and record transaction details, reduce information exchange exposure and eliminate the need for external validation--is desirable. Blockchain can do all of this, and more.

This paper introduces blockchain technology, describe payment card processing and blockchain use within the payment card processing. Constraints and risks, along with ethical implications, close the paper.

2 Blockchain

The blockchain is a distributed digital ledger technology introduced by Satoshi Nakamoto in a paper published in 2008 called “Bitcoin: A Peer-to-Peer Electronic Cash System [6]. Nakamoto’s paper introduced a system of cryptocurrency called “bitcoin.” Bitcoin generates electronically, and every transaction using a Bitcoin records to a digital ledger, and open to updated by anyone involved in the transaction. Bitcoin is known as a peer-to-peer digital currency system that operates without any trusted intermediary, (not centralized, no Government oversight) [6]. Nakamoto designed blockchain technology as a separate module within the Bitcoin specification, which means designers apply the technology to other uses outside of Bitcoin. Blockchain, as the distributed digital ledger, does not store in a single physical location but disperses over a network of interconnected computers. All participants have a full copy of records. Cryptography and digital signatures allow each participant to manipulate the ledger without incurring security issues. Transactions and the encryption and recording of transaction details is the core of the blockchain process.

In the initial 2008 specification, Nakamoto describes three key technical tenants of blockchain [6]:

1) Maintain a Replicated Ledger: Record a history of all transactions details, append-only with immutable past transactions, and can replication and distribute to all participants.
2) Cryptography: Use of cryptography in the ledger to guarantee the authenticity of the transactions, the privacy of the transactions and confirms the identity of the participants.
3) Consensus Logic: Based on logic using a decentralized protocol (Merkel Tree) which can tolerate disruption and pruning while running, and fervently validating all transactions.

Based on these tenants, blockchain provides a linked list built with hash pointers used to encrypt and record transactions in a structured manner [6]. It is a decentralized and distributed, thus available to all participants who participate in a transaction. Its integrity lies with a full network consensus of the history of the transaction ledger. Transactions cannot alter without the consensus of all other nodes in the network--distributed validation at work. If a majority of participants agree on the validity of a block of pending transactions, it adds to the blockchain.

The blockchain enables the execution of a transaction without having to integrate or handoff to a third-party to verify participants or transaction details, thereby diminishing risk and processing time.

2.1 Replication Ledger: Blockchain Data Structure

The blockchain data structure is time stamped, non-repudiable transaction list of the entire systems history. Blockchain utilizes a distributed network of nodes that stores and maintains a copy of a "public ledger" containing a full list of transactions (Fig. 1) [6]. A group of these transactions referred to as a "block," are encrypted and added from top-to-bottom in the order that they occur [5]. A block adds to the end of each "chain" [4]. Once a block adds to the chain, it becomes a permanent record and data in that block is never modified. Blocks are connected through hash[3] chaining, utilizing[4] a cryptographic hash.

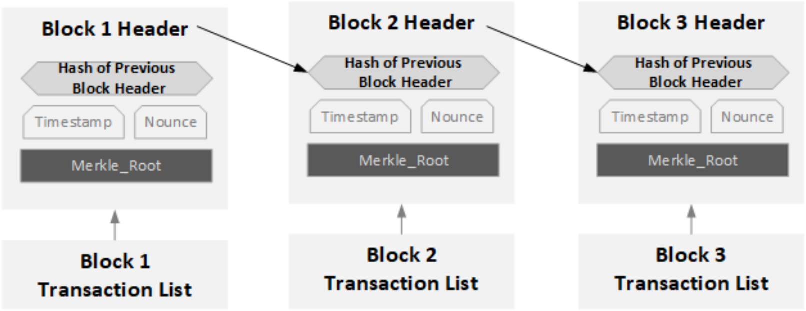


Fig. 1. Blocks connect through hash chaining. Blocks contain a header; headers chain, therefore blocks chain. The Merkle root relates the transactions in the block to the header, creating a logical combined unit. Blockchain does not allow an arbitrary block to attach to an arbitrary header. Each header only attaches to one set of transactions.

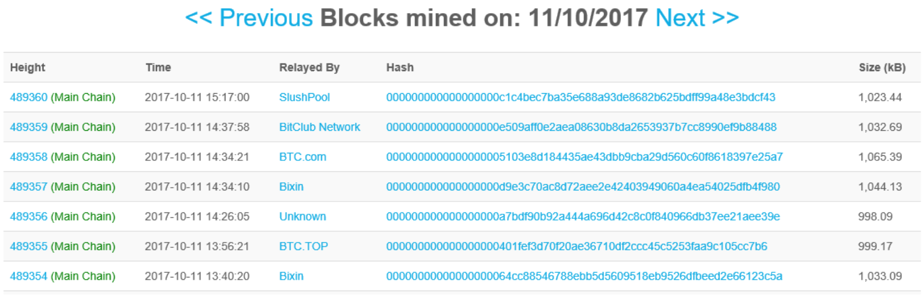
[3] The hash function takes any digital media and runs an algorithm on it to produce a fixed length unique digital output known as a ***hash*** [8].

[4] A cryptographic hash is hard to invert, and is therefore a member of the set of one-way functions [8].

2.2 Cryptography: Cryptographic Hash

The blockchain is a linked list built with hash pointers to record groups of transactions in blocks. The cryptographic hash function takes a variable size input text and returns a fixed size alphanumeric output called a “hash value.” Input text in blockchain is the header of the previous block and therefore chained. Hash values are irreversible, in that there are not enough known compute resources available to generate the original text from the hash value.

Every block in a blockchain is identified by a cryptographic hash, which identifies and maintains the integrity of the chain [7] (See example in Fig. 2). Every block contains a hash pointer to the previous block, after the genesis block (first block). The root hash pointer (Merkel Root) is a pointer to where the block stores. The pointer references the cryptographic hash of the entire block.



<< Previous Blocks mined on: 11/10/2017 Next >>

Height	Time	Relayed By	Hash	Size (kB)
489360 (Main Chain)	2017-10-11 15:17:00	SlushPool	000000000000000000c1c4bec7ba35e688a93de8682b625bdff99a48e3bdcf43	1,023.44
489359 (Main Chain)	2017-10-11 14:37:58	BitClub Network	000000000000000000e509aff0e2aea08630b8da2653937b7cc8990ef9b88488	1,032.69
489358 (Main Chain)	2017-10-11 14:34:21	BTC.com	0000000000000000005103e8d184435ae43dbb9cba29d560c60f8618397e25a7	1,065.39
489357 (Main Chain)	2017-10-11 14:34:10	Bixin	000000000000000000d9e3c70ac8d72aee2e42403949060a4ea54025dfb4f980	1,044.13
489356 (Main Chain)	2017-10-11 14:26:05	Unknown	000000000000000000a7bdf90b92a444a696d42c8c0f840966db37ee21aee39e	998.09
489355 (Main Chain)	2017-10-11 13:56:21	BTC.TOP	000000000000000000401fef3d70f20ae36710df2ccc45c5253faa9c105cc7b6	999.17
489354 (Main Chain)	2017-10-11 13:40:20	Bixin	00000000000000000064cc88546788ebb5d5609518eb9526dfbeed2e66123c5a	1,033.09

Fig. 2. Blockchain Blocks mined, reported to blockchain.info. Note the hash. Source: blockchain.info, extracted 10/11/2017 from https://blockchain.info/blocks.

The original text cannot change without resulting in a change to the hash value. The same hash value cannot duplicate, even when using identical input text. Thus, the content of a transaction always obscures because the hash value serves as the referential point back to the block, vice the content itself. [8]. Additionally, data integrity of the original transaction automatically validates, as a change to the original text forces a change to the hash value and this is detectable within the chain. A cryptographic token is used as a secure and authenticate a transaction participant. A cryptographic token can be a digital signature and is used to verify a transaction is initiated only by the token’s rightful owner. This approach creates an immutable block.

2.3 Consensus Logic: The Merkel Tree

Blockchain systems employ a peer-to-peer network, in that individual nodes/users of the system, are interconnected, with no single point of control. Therefore, no intermediaries or direct connection between participants involved in a transaction. In public blockchain, nodes can leave or join at any time. In private blockchain, nodes must be invited to join and can leave at any time with notification [9].

The Merkel tree is the consensus protocol used by blockchain and is an essential part of blockchain's data integrity. The Merkel Tree detects any changes to any data within a block, by rerunning the process for each transaction—and comparing the results to the original hash.

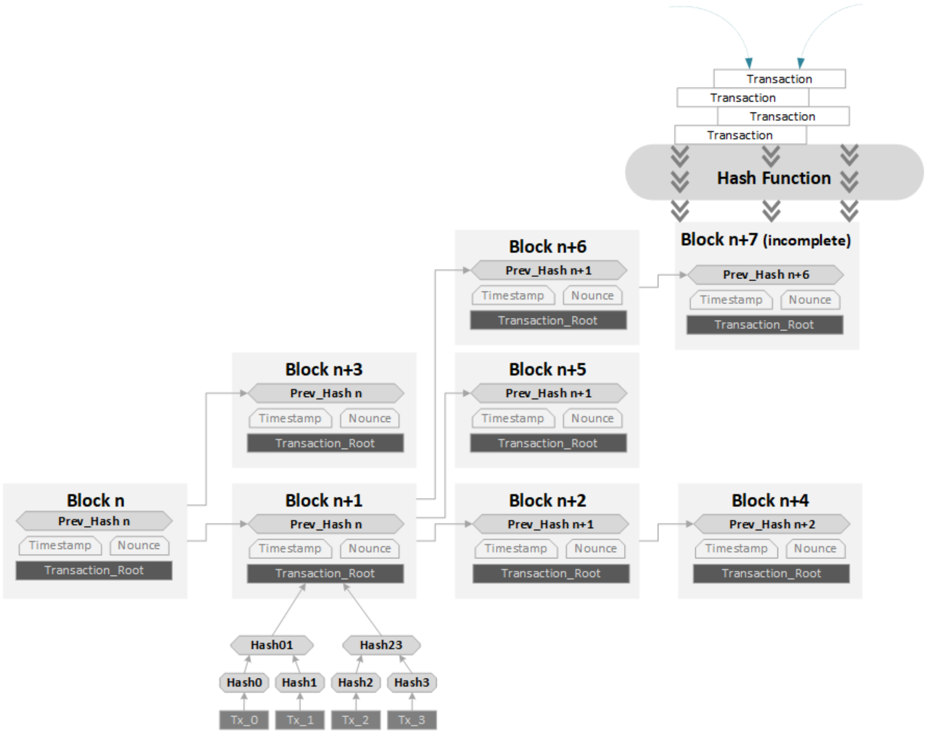


Fig. 3. Example of the applied blockchain. Blockchain uses a hash function for proof of work (mining) and data integrity (using Merkle Trees). All participants keep a copy of the ledger. The ledger divides into blocks containing many transactions. Blocks do not have to be in order, although transactions are [in the order created].

Transactions propagate across the network where the Merkel Tree consensus algorithms check whether a node copy of the ledger matches the copy of other nodes. This continuous verification circumvents falsification of data anywhere within the chain, and the process is known as a consensus protocol (Fig. 3) [10].

Each node keeps a copy of the block to give to other nodes when requested. Every block after that relies on that hash, and that hash relies on the Merkel Root, and the Merkel root relies on the hash of the transaction data. Altering the data within a chained block will cause that copy of the chain to no longer match the other nodes, thereby causing that node to be corrupt [6].

The Merkel Tree allows nodes with matching ledgers continue to process, while nodes with mismatched ledgers are marked as corrupt [11]. Transactions can be "pruned" from blocks, therefore removing the corruption.

Blockchain uses a cryptology that has yet to compromise. Additionally, blockchain ledger is comprehensive, that is, all transactions are traceable within a tree structure[5]. Data cannot corrupt because any alteration of the information on the blockchain would require an entire network override.

2.4 Public and Private Blockchain

The sole distinction between public and private blockchain is related to who can participate in the network, execute the consensus protocol and maintain the shared ledger [12].

In a public blockchain implementation, anyone can join, aggregate and publish transactions. When all nodes are not known, it is a "permissionless" blockchain [12]. A recognizable implementation of public blockchain is Bitcoin. Transaction data can be shared and stored immutably[6], and in the order in which it generates. Since the network reconciles every transaction[7] that happens within time intervals[8], data embeds within the network. This type of blockchain by definition is ***public***.

Public blockchains are considered to distribute and maintain more massive ledgers, thereby requiring more computation resources [12]. Additionally, public blockchains are open and inherently accept more security risks.

A private blockchain network requires an invitation and must validate by either the network operator or by a set of rules put in place by the network operator. Private blockchains give operators control over what nodes can read the ledger of verified transactions, can submit transactions, and can verify transactions, and reverse a verified transaction when necessary [10]. These characteristics enable a system that has faster transaction verification and network communication, the ability to fix errors and reverse transactions, and the ability to restrict access and reduce the likelihood of outsider attacks [13] [10].

When all writing nodes are known, it is "permissioned" or a consortium blockchain. Like public blockchain, data involved in a private blockchain can be shared and stored immutably, and in the order in which it generates. The difference is in the consensus process. Only selected nodes of the network reconcile every transaction that happens within time intervals. Data is thereby embedded within designated nodes of the network and is "private." Today, financial institutions, commodities trading, and private equity distribution are all testing private blockchain.

Application scope, usability, system security and the degree of transparency influence the decision to use private or public blockchain. Allison Berke, Executive Director of the Stanford Cyber Initiative, described the decision process akin to a network hosting decision, "Systems requiring fast transactions. The possibility of transaction reversal and central control over transaction verification is better suited for private blockchains. Those that benefit from widespread participation, transparency and third-party verification flourish on a public blockchain [10]."

[5] Blockchain uses single root hash forming a complete Merkle Tree.

[6] Immutably, immutable means that something is unchanging over time or unable to be changed.

[7] Communication occurs between nodes, each of which maintains a copy of the ledger and informs the other nodes of new information: newly submitted or newly verified transactions [10].

[8] For example, 10 minutes or as established by existing blockchain implementations used for Bitcoin transactions.

Although public blockchain is available for use, anyone can view and contribute to the ledger. This feature is not desirable in applications where sensitive data may be stored (such as financial records and personally identifiable information (PII)). Private blockchain (Permissioned) is desirable as control over participants, thus limiting information exposure. The blockchain can generate and establish trust among participants using encryption and digital signature technology.

3 Payment Card Processing

Payment card processing is the sequence of activities to complete a payment using a payment card. In the purest form, payment cards[9] transactions involve both a consumer and merchant participant, asset, agreed to form of currency exchange and a record of the transaction. Processing the transaction involves other vital participants such as the acquiring bank, issuing bank and a card scheme, for example, Visa or Mastercard or Discover Card[10] [14].

3.1 Payment Card Transaction Flow

A consumer can obtain a payment card by providing enough personal information to confirm his or her identity (they are whom they say they are) and the ability to fund purchases to an agreed to limit, at an agreed to rate[11]. Systems that process payment cards meet Payment Card Industry Data Security Standard (PCI DSS) information security standard, a standard required by most major credit card schemes[12]. PCI DSS compliance confirms systems can protect cardholder data and encrypt the transmission of cardholder data across open, public networks [15].

Using Fig. 4 as a reference, a financial transaction begins when a consumer initiates a purchase of an asset, and the merchant obtains a payment card from the consumer (cardholder). The merchant processes the purchase transaction using a payment card, and the authorization and funds verification steps initiate.

The consumer or cardholder's information associated with the payment card transfers to a payment gateway which in turn, routes the information to a payment processor. The payment processor submits the authorization for payment request to the issuing card's network.

[9] Payment cards are debit and credit cards. Payments using a debit card are immediately transferred from the cardholder's designated bank account, whereas credit cards pay the money back later.

[10] The card issuer is financial institution which issues the bankcard to the cardholder; the acquiring bank is the financial institution that pays the merchant bank for a card transaction [14].

[11] Financed using agreed to borrower's interest rates and terms.

[12] PCI DSS is not required by federal law in the United States. However, major credit card entities require PCI DSS compliance to participate in financial transactions [15].

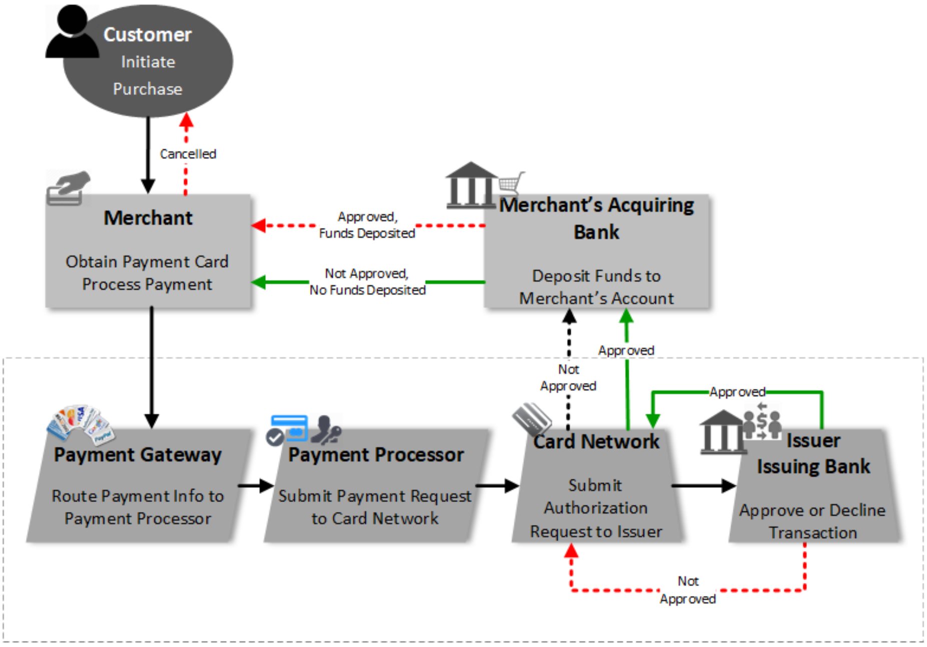


Fig. 4. The high-level process flow of a payment card transaction.

The authorization step validates the card security features (identity and authenticity of the cardholder). Authorization failures result in declined payment cards. The issuing card network submits authorization for payment to the issuer along with the status of the authorization step, and the issuer either approves or declines the transaction and notifies the card network.

The card network sends the authorization and issuers approve or decline status to the merchant's bank. The merchant's bank accepts or declines the transaction. Upon acceptance, it deposits receivables details into its account and submits the transactions to the issuing card's network. The issuing card's network pays the merchant, and charges the consumer's bank, and posts the transaction(s) to the cardholder's account. If the card declines, the merchant notifies the customer and cancels the transaction.

The Payment Gateway, Payment Processor, Card Network and Issuing Bank (boxed in Fig. 4) inherently require many information transmittals and state verifications just to complete a single payment card transaction. Card declines, and reversal of transactions require additional steps. Each step records to a separate log associated with one of these entities. Attempting to mine historical details of a transaction requires multiple requests to multiple ledgers systems to get an end-to-end representation.

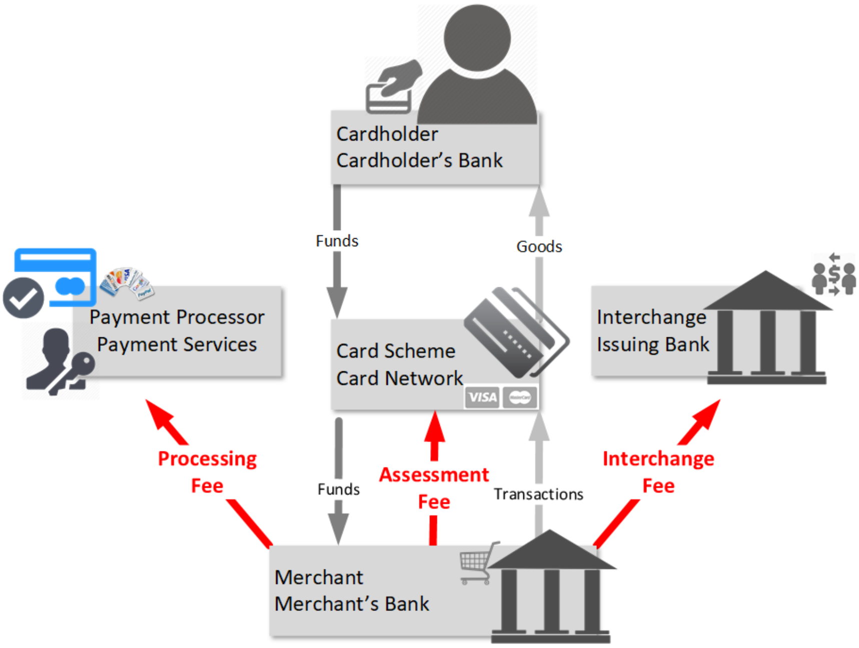


Fig. 5. The Cardholder submits a payment card for the purchase. The funds eventually make its way to the merchant, minus assessment fees, interchange fees, and payment processing fees.

The merchant is responsible for compensating third-party processors and validators in the form of fees. Fees apply to both accept a card and process it for payment. (see Fig. 5). A payment processor receives a percentage of the transaction value for handling the transaction. The issuing bank receives compensation for supplying the payment card to the consumer (cardholder). The payment card scheme/card network (e.g., Visa, Mastercard) receives a percentage of the transaction for making it possible for the consumer to utilize the payment card with the merchant [16]. The merchant pays the fees out of the total worth of the transaction, for accepting card payments. The compensation fees range from less than 1% up to 5% per transaction. Using a $100 transaction value as an example, this leaves the merchant with an estimated $97.87 deposit for a $100 transaction value. In general, fees incurred to cover the cost of performing the transaction. Given the number of entities involved in the steps shown in Fig. 4, the fees often qualify as processing and service availability fees.

3.1.1 Information Loss and Invalid Transactions

The cardholder must forgo private identification information one time to obtain and activate the card. However, PII information transfers to third-party payment card processors and verifiers over the life of each transaction. PII information can transfer a minimum of three times (Fig. 6). Information transfers take place over a network. Scanners, other wireless intrusion systems, embedded software viruses, and illegal hardware intercept devices can extract transaction details, thereby creating a condition of information spillage. The higher the number of external information transfers, the higher the rate of exposure, and the higher the risks of PII spillage. PII spillage is a *loss* to the cardholder.

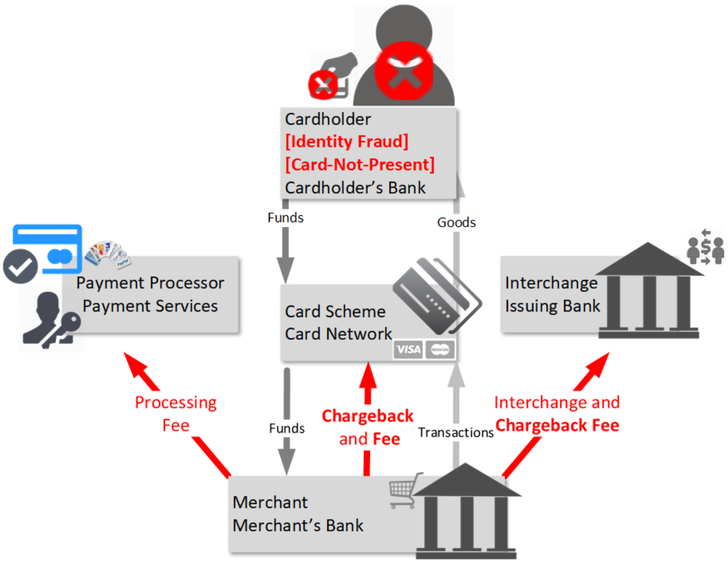


Fig. 6. The Cardholder submits a payment card for the purchase. The funds eventually make its way to the merchant, minus assessment fees, interchange fees, and payment processing fees.

Illegal or invalid transactions (fraud) that take place on behalf of the cardholder, without the permission of the cardholder results in loss of funds and incurrence of recovery fees. Cardholders are protected from the financial liability of unauthorized credit card transactions by Regulation Z [13] of the Truth in Lending Act and unauthorized debit card transactions by Regulation E[14] of the Electronic Fund Transfer Act. Card schemes (associations) have a set of fraudulent transaction rules which define chain-of-liability to determine who is responsible for making compensations to the cardholder. Compensation is known as "chargeback."

In cases where chargebacks result from *card-not-present* transactions, the issuing bank recovers the funds from the merchant's bank (the acquiring bank), and the acquiring bank recovers the funds from the merchant. Chargebacks do not occur within the period of the transaction, but often many weeks or months after. The risks of the acquiring bank recovering the funds are higher as more time passes. At times, a merchant is no conducting business or has suffered a financial loss to the degree they cannot pay. The Merchant's inability to pay the chargeback forces acquiring banks to write off the full amount of the chargeback as a loss. Of course, the chargeback

[13] Glossary Term.

[14] Glossary Term.

process incurs fees, and the merchant must also pay these fees, which compounds the overall financial loss to the merchant [17].

Another case of fraud is termed *buyer identity fraud*. Buyer identity fraud occurs when a customer uses a stolen payment card (or one established using a stolen identity) to purchase a product from a merchant. Many card schemes require Merchants to cover chargebacks resulting from buyer fraud [17]. Assets exchange and the fraudulent buyer often has possession of the assets, thereby causing a merchant loss of assets, funds, and fees to process the loss.

There are many other cases of fraud, for example, the cardholder intentionally attempts to defraud a Merchant (*friendly fraud*), or where a Merchant attempts to fraud the customer (*Merchant fraud*). In all cases, chargeback and fee structures apply.

4 Using Blockchain for Payment Card Processing

4.1 Cardholder Identify Verification

Fig. 7 depicts the cardholder identity verification steps involved in a payment card transaction. As Fig. 7 shows, the authorization is a multi-step process involving multiple third-party entities.

Private blockchain uses an existing digital identity verification technology known as public key cryptology. Public-key cryptography algorithms use digital signatures to validate a person has the right key to sign digital assets and prove they are whom they say they are. Two keys are essential, a private key and a public key. The private key is kept private and is only used by the owner. The public key is a mathematical key related to the private key and used to verify a transaction was indeed signed using the private key. Anyone who needs to verify ownership claims shares the public key.

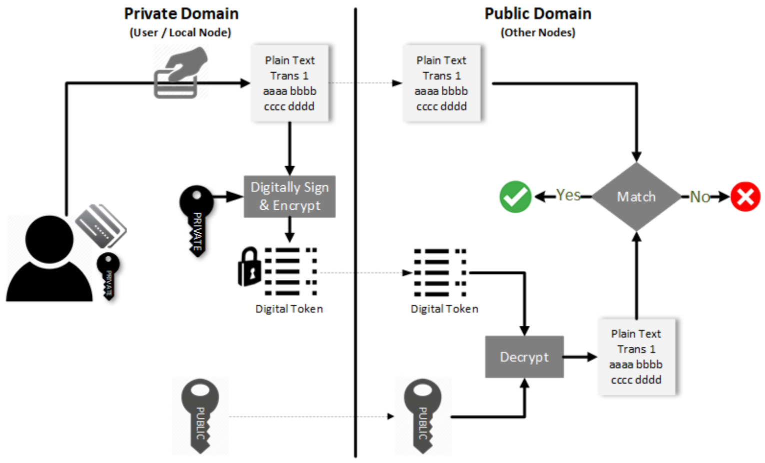


Fig. 7. Steps of Identity Verification Using Public Key: 1. The Cardholder submits a payment card for purchase, and signs with the private key (pin number), and creates a digital token. 2. The digital token and a public key are sent to the merchant's bank to verify the cardholder. 3. The merchant's bank verifies the digital token using the cardholder's public key.

Cardholder verification would consist of a private key generated for the card and used by the user to digitally sign a transaction, which creates a digital token. The public key stored on the payment card. The merchant banks receive the digital token (transaction details) and utilize both the public key and private key to verify the cardholder and the transaction.

An adjustment can technically be made to the blockchain ledger to include a full trace or period trace of the payment card transaction history from the time the card was dispensed or activated to the cardholder through to the most recent purchase history, each time the cardholder submits the card in a transaction

4.2 Payment Card Terms and Funds Authorization

Private blockchain can replace the need to authorize funds by storing a full trace of the payment card history (all transactions) either on the card in an embedded chip or referenced by an application pointing to information in the cloud. Available funds and card terms refresh when the card submits for the next transaction (pushed) or when the next scheduled periodic update occurs (pull). Period updates are configured by the cardholder within an application or using a web-based payment card processing system.

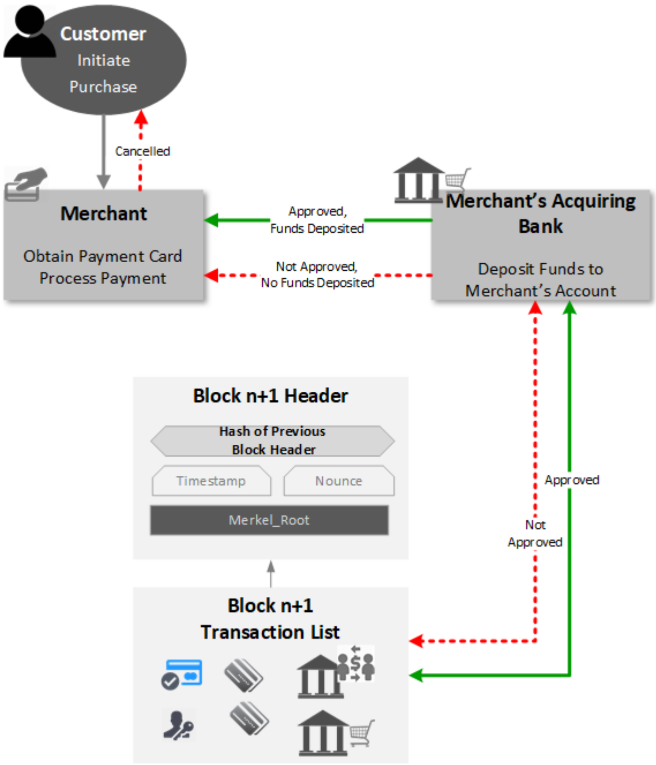


Fig. 8. High-level transaction flow using blockchain to store card and cardholder information required to authorize funds for most transactions.

When a cardholder submits the payment card for a transaction to the merchant, the merchant's local payment processor can immediately determine if the transaction can complete within the boundaries of the payment card terms. The terms, authorization state, and available funds store to a blockchain transaction ledger (list), along with the date the information was last updated (Fig. 8 and Fig. 11). The data may trigger an automatic refresh (pull) if the available funds and terms information are outside of an established refresh period.

Issuing banks and merchant bank terms may include a minimum information refresh period requirement, where cardholder authorization, card authenticity, available funds, terms are confirmed within a specified period—refreshed within the last 24 hours, for example. The issuing bank determines update iterations. The issuing bank may own the mobile application and data refresh terms would specify periodic update requirements. Periodic updates essentially reflect how current the funding information must be.

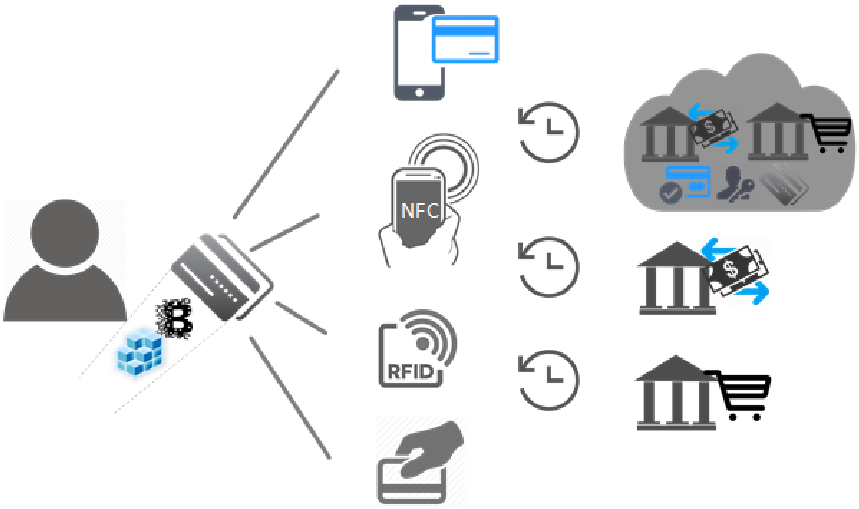


Fig. 9. Payment card information can update in a variety of ways, including mobile applications utilizing cloud locations, or RFID and NFC interfaces to merchant applications.

Mobile technology provides an additional level of convenience and can be designed to support both push and pull updates. Mobile applications using, cloud-based information drop points, can be used to post updated information to a cloud location (push) (Fig. 9). Thus making it ready for download via the app or other communications interfaces such as Radio Frequency Identification (RFID)[15] and Near-field communication (NFC)[16] when activated (pull) (Fig 8). Updates can be retrieved and added to blockchain ledger transaction list when the cardholder next establishes a link to a cellular or wireless (WIFI) network. Cardholders can configure their mobile preference settings for application network requirements (such as cellular on/off; WIFI only for update).

4.2.1 Cash Withdrawals

Cash withdrawal transactions are not a form of payment, but can also be supported using blockchain: available funds information and terms are already known and fresh and available in the blockchain transaction list. A cash withdrawal would merely use the available fund's information, and update the blockchain transaction for a confirmed withdrawal, as well as the newly available funds after withdrawal.

[15] RFID systems are short range read distance technologies measured in inches of communication distance.

[16] Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device.

4.2.2 Delayed or Offline Processing

In the event a network connection is not available, technologies such as RFID and NFC can be used to complete a payment card transaction. For example, a cardholder submits a card for payment and enters a PIN in a merchant payment application to unlock the encrypted data on the card. The application can update the information between the cardholder's bank and the payment card itself. This technology eliminates the need for an internet connection, thereby giving the cardholder additional time to connect to a network and receive an update, but still complete a payment.

In the event a network connection cannot be established for an extended length of time, offline processing can utilize an existing blockchain payment technology known as "Zerocash," which relies on zero-proof authorization [18]. Payment card information, available funds and terms and zero—proof authorization combine to enable a payment card transaction to complete offline.

The blockchain ledger can include as much information necessary to reflect the credentials of the consumer, the issuing bank and the available funds associated with the cardholder's bank as embedded information stored in the blockchain transaction list.

4.2.3 Adjustments to Merchant Payment Applications

Merchant Point of Sale (POS) systems adjusts to "mine" the blockchain transaction list from the card, to obtain information to authorize and approve a transaction. Rather than making three to four information requests and exchanges with third-party validators, a single mining request completes locally, using a merchant application and interface.

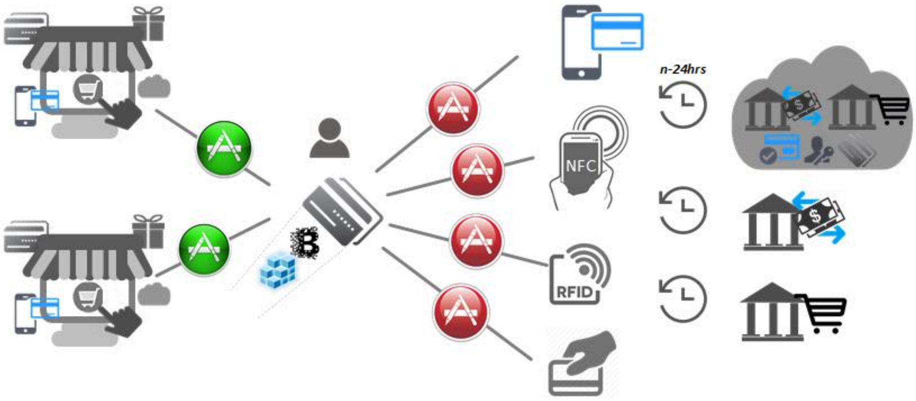


Fig. 10. Merchant Applications adjust to accept blockchain smart payment cards.

Security credential and personal identification information are mined to initiate cardholder identity verification and card scheme information.

4.2.4 Security

New technologies present new challenges to security schemes. Data encryption helps guard against those attempting to steal data using scanners (RFID), or other methods. Data resides as encrypted private blockchain. All of these methods help prevent passer-by skimmers from easily downloading data to a device via RFID, for example.

NFC devices are another form of technology which can help secure the payment card. RFID (Radio-frequency identification) concepts are the basis of NFC technology, which relies on electromagnetic induction to transmit information. NFC active devices both send and receive data and can communicate with each other, as well as with passive devices. Smartphones are the most common implementation of active NFC devices. Public transit card readers and touch payment terms also use NFC technology [19].

As for cardholder identity, blockchain and payment card systems already use a public-key cryptology technology for identity verification. This technology is not new, but heavily used in many industries.

4.3 Example of Payment Card Processing Using Blockchain

A notional payment card flow using blockchain is in Fig. 11. A consumer (cardholder) submits a payment card to a Merchant as payment for a good or service. The Merchant accepts the payment card by inserting the card to a POS hardware chip reader device. Security verification processes commence. The Merchant POS system mines the *authentication markers, authorization IDs, biometric indicator, public key,* and *private key* from the blockchain to complete security verification. All information transfers are between the POS system and POS chip reader (local).

The POS system also mines issuing bank verification information such as *bank authorization identifiers* (two possible), *card rate* (percentage rate), *spending cap* or *terms,* and the *card activation date*. These details confirm the bank and that the card is active. Information transfers are again, local and between the POS and POS chip reader device.

The POS system verifies the currency of card payment information by mining the most current *update date,* from the blockchain, to determine if the card terms are within a pre-defined window of time (e.g., 24 hours). Each update appends the blockchain with *card rate, card terms, update date* (MMDDYY), *available funds* and logs the *ten most recent transactions* to the blockchain.

When a digital transaction is carried out, it groups in a cryptographically protected block with other transactions that have occurred in the last 10 minutes and sent out to the entire network [20]. Therefore, an update occurs within the same block if the transaction time spans less than 10 minutes. If more than 10 minutes, a new block appends to the chain (Fig. 11, *Block n1*). Most payment card transactions occur, in full, within two minutes, and transaction details will more than likely, record to one block.

The *Merchant's key* records to the blockchain. The POS application updates the *Merchant's key, Authorize Transaction state* indicator to 01 (approve), 00 (do not approve) or 99 (force refresh) based on payment card terms from the blockchain if the information deems current. The approval or disapproval indicator confirms or denies that available funds cover the amount of payment to the Merchant, or that *available funds* term is of age, and needs to refresh. Indicators do the following:

- 01 Approve: The *Authorize Transaction state* indicator reflects 01 or "approve" code if the blockchain transaction list reflects a recent update to card terms and available funds (within the last 24 hours or predetermined window of time), and the available funds do back the payment amount.
- 01 Disapprove: The *Authorize Transaction state* indicator reflects 02 "disapprove" code if the blockchain transaction list reflects a recent update to card terms and available funds (within the last 24 hours or predetermined window of time), and the available funds cannot back the payment amount. If a 00 does appear in the *transaction state*, the transaction terminates and sends a message to the Merchant POS application. The Merchant then notifies the cardholder that the transaction is canceled/rejected.
- Force Update: The *Authorize Transaction state* indicator reflects "force update" or a 99 code if the blockchain transaction list reflects that the last update to card terms and available funds were outside of the period (within the last 24 hours or predetermined window of time). If the information is of age, the POS system sends a request to refresh to the issuing bank. This request adds the most recent *card rate*, *card terms*, *update date* (MMDDYY), *ten most recent transactions* and *available funds* to the blockchain.

The *payment bank* (bank number) and *payment amount* also update the blockchain.

Each time the cardholder submits the card for payment, this process repeats. The entire chain is continually updated so that every ledger in the network is the same, giving each [20] transaction participant the ability to prove transaction information what at any given time.

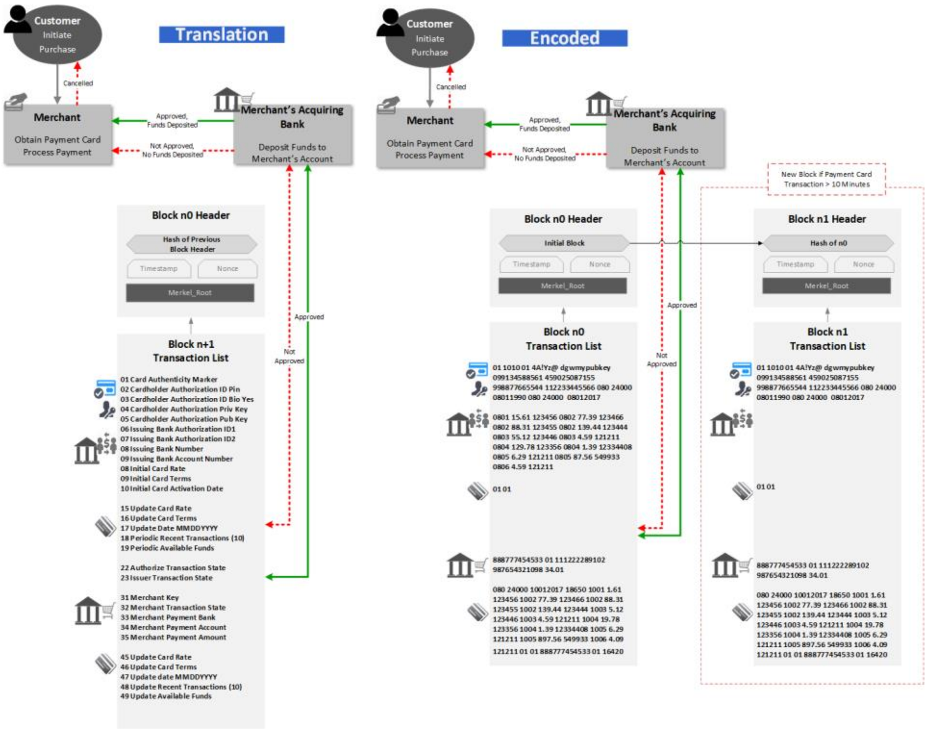


Fig. 11. The full notional process flow of a payment card transaction has been restructured to show the use of blockchain. Data is encoded (right diagram) and references various pieces of information (left diagram) related to a payment card transaction. Block *n1* (rightmost block) only creates if the transaction spans more than ten (10) minutes.

4.4 Benefits of Using Blockchain

Reduce Transaction Participants

The use of private blockchain within payment card processing reduces the number of participants to only those active in the immediate transaction. Transaction details are only viewable those participants. Participants can merely include the consumer/cardholder, merchant [POS], and merchant's bank. Notation: The *public* blockchain is not viable because participation is open to the public, and the transaction list available for anyone to view.

Reduce Transaction Processing Time

Overall payment card transaction time reduces by removing the need for third-party information exchange and approval steps (Fig. 12). Information exchanges take place between the payment device and POS application by mining the blockchain. While present compute resources are designed for performance and speed, reducing the overall transaction time is still a desirable goal for any application.

Risks associated with disclosing sensitive information go away because the number of external information exchange points (or network transfers) shrinks.

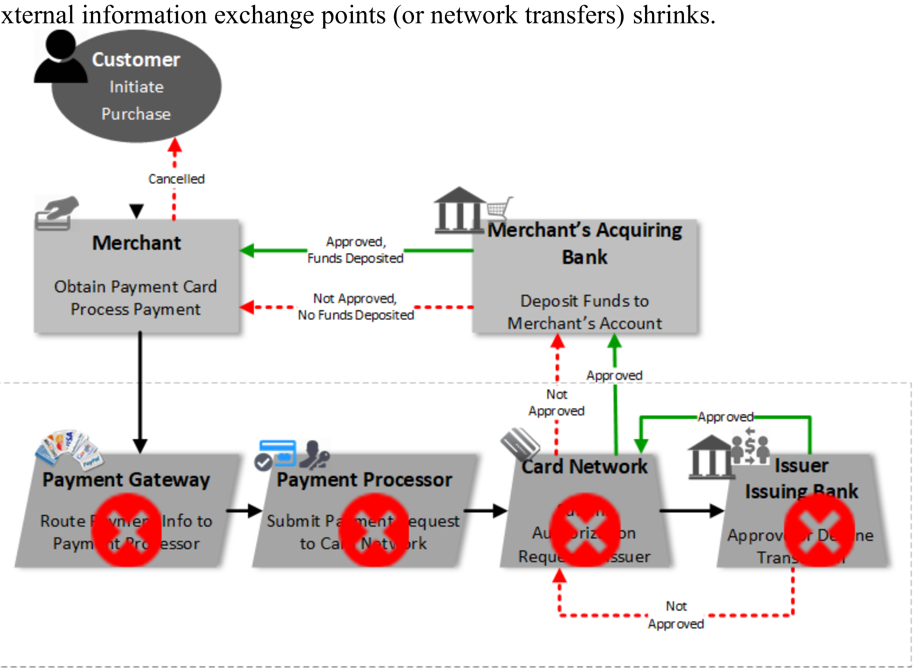


Fig. 12. The high-level process flow of a payment card transaction has been restructured to show the use of blockchain. Fewer parties participate, associated transaction ledgers and excessive information transmittal and state verification steps. Enough information to validate the authenticity of the card, cardholder and available funds travels in the blockchain ledger, onboard the card.

Utilize a Single Encrypted Transaction Ledger

Removing the need for third-party validators also means transaction details exist in a single encrypted digital ledger or blockchains transaction list, vice details spread across multiple transaction ledgers.

Increase Data Integrity

The Merkel tree is the consensus protocol used by blockchain and is an essential part of blockchain's data integrity. The Merkel Tree detects any changes to any data within a block, by rerunning the process for each transaction—and comparing the results to the original hash. This kind of data integrity coupled with the use of a single transaction registry provides a single comprehensive source of truth for each transaction, operating within a robust encryption security wrapper.

Cardholder data involved in a private blockchain can be shared and stored immutably, and in the order in which it creates. The consensus process allows only selected nodes of the network to reconcile every transaction that happens within time intervals. Data is thereby embedded within designated nodes of the network and is "private." Private blockchain uses hash encryption for data. Hash encryption cannot be reversed, thereby protecting the identity associated with the payment card and details of a transaction.

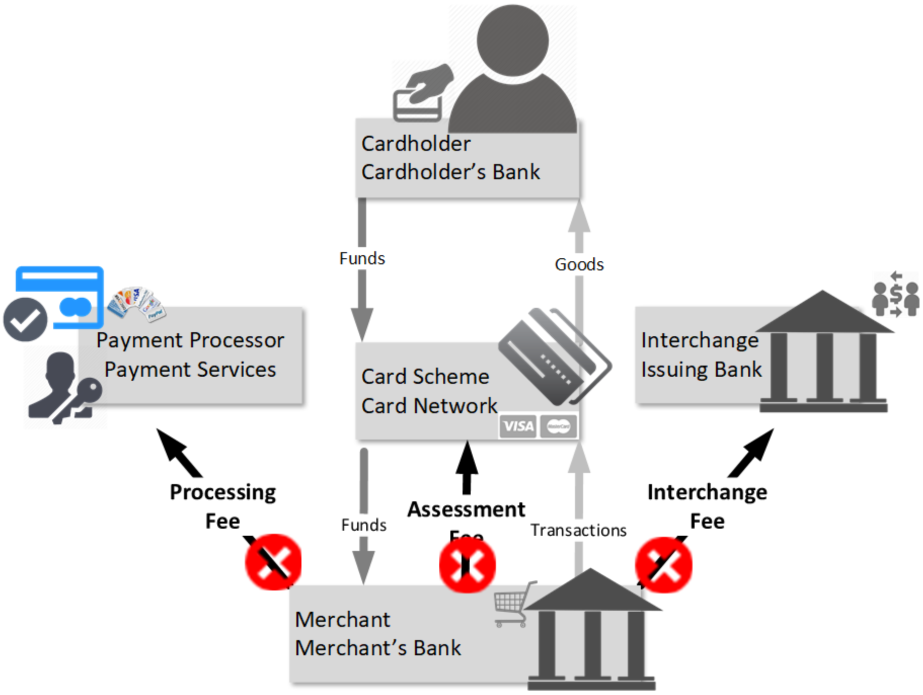


Fig. 13. Fees associated with existing payment card transactions can disappear or substantially reduce by using blockchain to store current and periodic information about the payment card and cardholder.

Reduce Transaction Fees

Fees associated with existing payment card transactions can disappear or substantially reduce by using blockchain to store current and periodic information about the payment card and cardholder. This onboard information is useful to both security and cardholder verification processing. Verification takes place locally between the payment card (insert to chip reading device) and the Merchant's POS system. With the relevant information residing in blockchain onboard the card, third-party verification is no longer necessary (Fig 13). Payment card refresh rates must apply to keep card terms in synch with issuing banks.

Unfortunately, fees associated with fraudulent transactions can only decrease by thwarting fraudulent activities, i.e., improving cardholder verification. Merchant payment acceptance policies and practice, and Merchant POS systems can adjust to using blockchains public-key and digital signature verification methods.

Additionally, the problem is not the payment processing systems alone. Peripheral systems which issue and activate payment cards are also culpable. Technologies like private blockchain can help to defend against fraud, but they cannot prevent it.

Conform to PCI DSS

Private blockchain supports helps satisfy PCI DSS requirements to protect a cardholder's information. Private blockchain's operator control of distributed ledgers [21] and encryption of transported data comply with the PCI DSS standards. Since private blockchains give operators control over what nodes can read, submit, verify and reverse transactions, it can restrict access and reduce the likelihood of outsider attacks.

5 Constraints and Risks

There are a few constraints and risks of introducing blockchain into the payment card processing systems and processes, and these are as follows.

5.1 Constraints

Imposed Delay: Achieving blockchain transactional consensus (of transaction viability) takes at least 10 minutes by design. Nodes continue to form before all transactions verify (ranging from 60 to 120 minutes to verify). If corruption occurs, by this time, an extensive chain is built, and forking a new version of the ledger could be expensive. The delay is a vulnerability of the system itself, and not suited to high-speed transactions [10].

Performance [Runtime Versus Real-time]: Fast transactions are a cornerstone of credit card processing. The speed of the transaction is essential because all identification, verification, and funds authorization step complete while the consumer waits. Blockchain must adhere to expected performance requirements.

Throughput: Large payment card systems process approximately 2,000 to 3,000 (est. 260 million per day) transactions per second. The most recent known blockchain systems process 367,000 a day (Fig. 14 and Fig. 15).

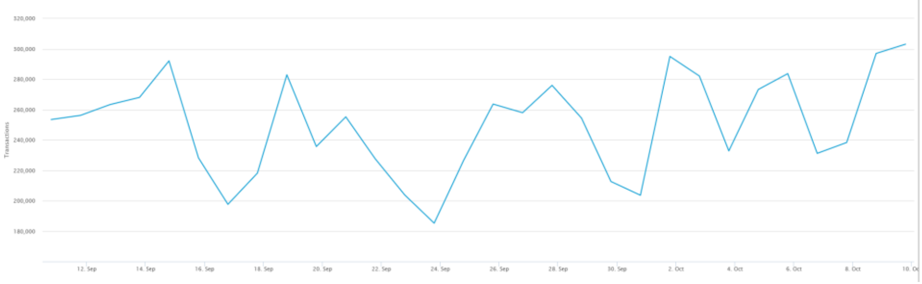


Fig. 14. 30-day record of All-Time record of blockchain transactions as recorded by blockchain.info. Source: blockchain.info, extracted 10/11/2017.

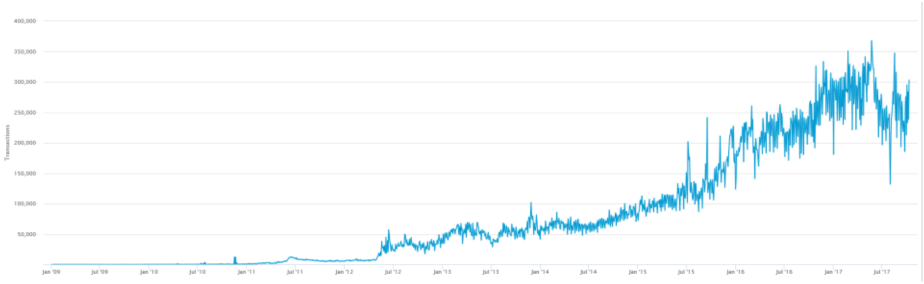
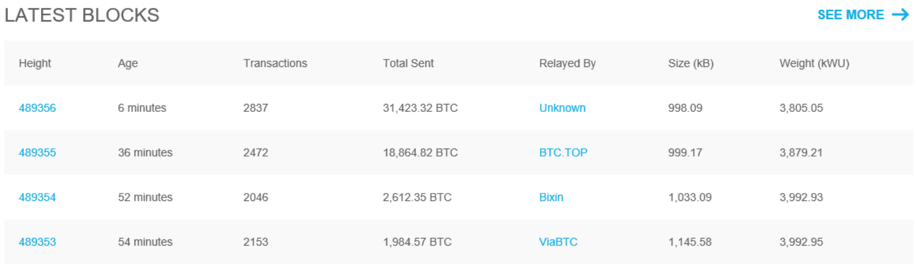


Fig. 15. The record of blockchain transactions as recorded by blockchain.info. Source: blockchain.info, extracted 10/11/2017.

Adoption: Mainstream financial institutions (acquiring banks, issuing banks, card networks) would have to adopt blockchain systems. This kind of modification could take years, although some work has begun [7].

Limited Block Size: Current implemented blockchain systems, used for cryptocurrency exchange, have an imposed size limit of 1 megabytes (MB) [6]. This size limitation is intended to limit the number of transactions that process within a block. Blockchain systems must adjust the maximum block size, or force a limitation on the total number of transaction writes to a block for a full transaction sequence. Fig. 16 is a posting of blocks for October 10, 2017. Blocks near 1MB contain roughly 2,100 to 2,800 transactions. Changing the block size can introduce performance concerns, as huge blocks could impact network throughput rates. Blockchain can prune nodes that are too large, however, the impact of pruning forces additional mining for those seeking a full transaction history.


LATEST BLOCKS

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
489356	6 minutes	2837	31,423.32 BTC	Unknown	998.09	3,805.05
489355	36 minutes	2472	18,864.82 BTC	BTC.TOP	999.17	3,879.21
489354	52 minutes	2046	2,612.35 BTC	Bixin	1,033.09	3,992.93
489353	54 minutes	2153	1,984.57 BTC	ViaBTC	1,145.58	3,992.95

Fig. 16. Latest Blocks Posted to Blockchain. Info 10/11/2017. Source: blockchain.info, extracted 10/11/2017.

Card Storage: Payment card chips would have to adjust to contain pertinent blockchain information and execution triggers for periodic updates to payment card information.

5.2 Risks

Lost or Stolen Credentials: Lost identification credentials, particularly for systems that manage physical assets, cannot recover stolen assets because ownership cannot be proven. Transactions submitted with stolen keys appear to a verifying node to be indistinguishable from legitimate transactions [10]. Reverse a verified transaction is the only recourse, but costly and another potential risk. Transaction reversal can undermine confidence in the fairness and impartiality of the system.

Network Availability: Uncommunicative nodes or intermittently active nodes go offline for various reasons, and when they do, the network architecture must be such that the network continues to operate with offline nodes and self-correct when possible.

Network Integrity: A node that restricts the transmission of information, or transmits incorrect information, must be identifiable and circumventable to maintain the integrity of the system [10].

Quantum Computing: Quantum computing has the potential to outperform classical supercomputers. The encryption algorithm known as Shor's algorithm may render the RSA cryptosystem unsalvageable. Shor's algorithm is considered to be faster than both. Additionally, the larger the RSA "key" — the number that must be factored — the greater the speed difference. The authors of the paper estimate that attacking a terabyte-size key using Shor's algorithm would require around 2100 operations on a quantum computer, an enormous number [22].

Trust: Private blockchains can manage the assignment of nodes, and allocate some to perform the verification process. Assigning this level of trust (securing nodes and trusted party) introduces an operational security risk.

6 Conclusion

Blockchain has the potential to satisfy requirements for protection of sensitive information within a transaction. However, to be useful, it must transform or extend to the degree that it can be applied, and implemented by mainstream issuing banks, acquiring banks and endorsed by card schemes, payment processors and card networks.

The private blockchain is the most viable form of the blockchain, given private blockchain allows elements of control over the consensus process (who can operate a node and how the nodes are connected), which helps mitigate inherent risks. Blockchain encryption technology is not new and has been used extensively in other systems, so the risk of introducing new technology failures is low.

A payment card transaction involves four to five information exchanges between payment processors, payment gateways, a merchant's acquiring bank and the card issuing bank. The exchanges authorize the identity of the cardholder, verify available funds, card terms, and authorize payment to the merchant's account. Risks of information exposure increase exponentially with each exchange point. Each entity captures transaction details. Fees are incurred by the merchant to cover the costs of processing a payment card transaction.

Payment card processors and banks capture transaction details in separate loosely associated registers. Blockchain can record every detail of a transaction in an encrypted single digital register. The digital register substantially reduces the number of queries needed to view full cycle transaction details.

Blockchain can reduce information exposure by reducing the number of exchanges required to verify and validate cardholder and payment card details. Blockchain can reduce the number of validation points, by allowing payment card information to reside on the card as encrypted data resident in the transaction list. Because blockchain is a single encrypted digital register, it substantially reduces the effort required to mine transaction details. Blockchain data can include all details associated with the cardholder, card terms and issuing banks available funds. Verification and validation steps disappear if using blockchain, thereby reducing the risk of information exposure and reducing the cost to a merchant by eliminating processing fees.

There is no question that blockchain introduces a smarter ledger technology, with inherent security characteristics desired by many. However, any hesitancy to accept blockchain in mainstream practices is related more to the investment required to adjust mainstream banking systems. For example, at a minimum:

1) Redesign payment card architecture to allow blockchain on card in the card-based computer chip;
2) Redesign merchant POS systems and POS chip readers to accept and mine blockchain based payment cards;
3) Redesign card authentication and authorization verification systems to mine card-based verification information from a blockchain;
4) Redesign account verification systems to mine card-based verification information from a blockchain;
5) Significantly reduce or remove processing and service availability fees related to accepting and using payment cards.

These kinds of adjustments require extensive investment. While there is hesitancy, some banks are already investing in blockchain technology for financial asset tracking, contract management, and investment banking. The adoption of the technology is expected to only increase in the coming years [23], and perhaps this can include payment card processing.

7 Ethical Discussion

As with all new technologies, the concern of ethical considerations exists. Blockchain specifications strongly proport tight security, because blockchain utilizes a series of cryptographic hash codes to record transactions. The approach also provides a degree of inherent privacy for participants—if using private blockchain. Blockchain also provides built-in integrity; all transactions interrelate through backward and forward block chaining. Even with the sophisticated approach to encryption and chaining, blockchain is still prone to hacking attempts.

Since the initial release of Bitcoin using blockchain, hacking attempts against frequently occur in an attempt to discover the identity of Bitcoin transaction participants. For example, in a paper by Peter L. Juhasz ("A Bayesian Approach to Identify Bitcoin Users"), Juhasz describes his teams attempt to reverse engineer the blockchain registry. Juhasz's team uses a two-step approach to attempt to reveal transaction ledger details. Each transaction was associated with a client, using the clients IP address. Bitcoin addresses mapped to client IP addresses. A probability model was used to determine which pairings were most likely. The team, using the Bayesian method, ferreted the geographic location of each client based on IP address, and then conducted a spatial analysis of distribution and flow of Bitcoin." They were able to identify a client's location and associated transaction details. While this example pertains to Bitcoin, it demonstrates the kinds of methods to break the security features of the blockchain.

The value of information determines the threat of its exposure--the more valuable, the more attempts to gain access. Blockchain uses more sophisticated methods to secure and maintain the integrity of blockchain data, thereby creating a system less prone to information exposure.

Citations

[1] The World Bank, "Individuals Using the Internet," The World Bank, 16 July 2016. [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS. [Accessed 31 Oct 2017].

[2] S. V. A. G. W. Jason Kuruzovich, "Marketspace or Marketplace? Online Information Search and Channel Outcomes in Auto Retailing," Information Systems Research Journal, 18 July 2008. [Online]. Available: https://pubsonline.informs.org/doi/abs/10.1287/isre.1070.0146. [Accessed 11 Nov 2017].

[3] U.S. Government. FTC, "Glossary of Telecommuncations Terms," U.S. Federal Telecommunication Standards Committee, 10 Oct 2016. [Online]. Available: https://www.its.bldrdoc.gov/fs-1037/dir-032/_4768.htm. [Accessed 31 Oct 2017].

[4] R. Roth, The Value of Information. Dynamic Strategic Planning, Boston: MIT Press, unknown.

[5] National Institute of Standards and Technology, "NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," 4 2010. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-122/final. [Accessed 17 10 2017].

[6] S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System.," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 10 8 2017].

[7] S. &. A. S. Adarsh, "Chapter 2, Introduction to Blockchain Technology," in Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities, Hershey, IGI Global, 2014, p. 127.

[8] W. Stallings, in Cryptography and Network Security: Principles and Practice, 6th edition, Boston, Pearson Education, Inc., 2014, pp. 313-355.

[9] D. &. A. Tapscott, "What is Blockchain Technology? A Step-by-Step Guide for Beginners," 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. . [Accessed 10 8 2017].

[10] A. Berke, "How Safe Are Blockchains? It Depends, Harvard Business Review, Technology," 7 3 2017. [Online]. Available: https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.. [Accessed 6 10 2017].

[11] L. Cheng, "An Introduction to the Bitcoin Blockchain," 6 January 2015. [Online]. Available: http://insights.wired.com/profiles/blogs/the-bitcoin-blockchain-and-the-coming-tokenization-of-user.

[12] P. Jayachandran, "The Difference Between Private and Public Blockchain, IBM Blog," 31 5 2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/. [Accessed 6 10 2017].

[13] A. Banafa, "IoT and Blockchain: Challenges and Risks," Tech by LinkedIn , 16 Nov 2017. [Online]. Available: https://www.bbvaopenmind.com/en/iot-and-blockchain-challenges-and-risks/. [Accessed 23 Nov 2017].

[14] J. Slawsky and S. Safar, "Future of Payment Cards," in Developing and Managing a Successful Payment Cards Business, New York, Routledge, 2005, p. 159.

[15] PCI Security Standards Council, "PCI Security Standards.org," 2016. [Online]. Available: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf?agreement=true&time=1507830406359/. [Accessed 17 10 2017].

[16] D. S. Evans, " Chapter 1,"The Economics of Interchange Fees," in Interchange Fees: The Economics and Regulation of What Merchants Pay for Cards, CreateSpace Independent Publishing Platform, 2011, pp. 2-5.

[17] FDIC, "Risk Management Examination Manual for Credit Card Activities," FDIC- Division of Supervision and Consumer Protection 164, March 2007.

[Online]. Available: https://www.fdic.gov/regulations/examinations/credit_card/pdf_version/ch19.pdf. [Accessed 11 Dec 2017].

[18] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer and M. Virza, "zerocash-project.org," 18 5 2014. [Online]. Available: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf. [Accessed 17 10 2017].

[19] B. Nicoletti, "Glossary," in Nicoletti, Bernardo. The Future of FinTech: Integrating Finance and Technology in Financial Services, Boston, Macmillan, 2017, p. Location 5635 of eBook.

[20] M. v. Rijmenam, "What is the Blockchain and Why is it So Important?," Founder dscvr.it & Datafloq, September 5 2016. [Online]. Available: https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam/. [Accessed 11 Dec 2017].

[21] P. Kovary, F. Zhou and M. Adoul, "Blockchain Technical Details," [Online]. Available: http://www.doc.ic.ac.uk/~ma7614/topics_website/tech.html.

[22] M. H. Kim, "Why Quantum Computers Might Not Break Cryptography," 17 May 2017. [Online]. Available: https://www.quantamagazine.org/why-quantum-computers-might-not-break-cryptography-20170515/. [Accessed 6 Dec 2017].

[23] Raconteur, "The Future of Blockchain in 8 Chart," 27 6 2016. [Online]. Available: https://www.raconteur.net/business/the-future-of-blockchain-in-8-charts.. [Accessed 10 8 2017].

[24] N. Popper, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money, Chicago: Harper; Reprint edition, 2015.

[25] Federal Telecommunication Standards Committee, "Federal Standard, Telecommunications: Glossary of Telecommunications Terms. FS-1037C.," 2016. [Online]. Available: https://www.its.bldrdoc.gov/fs-1037/dir-032/_4768.htm.. [Accessed 31 10 2017].

[26] National Institute of Standards and Technology, "NIST Special Publication 800-63, Revision 3, Digital Identity Guidelines, Appendix A—Definitions and Abbreviations.," 10 6 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed 17 10 2017].

[27] National Institute of Standards and Technology, "NIST Special Publication 800-78, Revision 4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification," 5 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPub. [Accessed 17 10 2017].

[28] Farlex, "The Financial Dictionary," Farlex, 2017. [Online]. Available: https://financial-dictionary.thefreedictionary.com/credit.. [Accessed 31 10 2017].

[29] Federal Trade Commission , " Banking and Financial Services," in Prepared Statement of The Federal Trade Commission Before the Subcommittee on Financial Institutions And Consumer Credit Committee On Banking And Financial Services on the Implications of Emerging Electronic Payment Systems on Individual Privacy, Washington, DC, 1997.

[30] A. Lewis, "A Gentle Introduction to Immutability of Blockchains," BitsonBlocks.net, 29 2 2016. [Online]. Available: https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/. [Accessed 6 10 2017].

[31] Board of Governors of hte Federal Reserve System, "Compliance Guide to Small Entities; Regulation E: Electronic Fund Transfers," Federal Reserve , 28 December 2016. [Online]. Available: https://www.federalreserve.gov/bankinforeg/regecg.htm. [Accessed 11 Dec 2017].

[32] Board of Governors of the Federal Reserve System, "Compliance Guide to Small Entities; Regulation Z: Loan Originator Compensation and Steering," Federal Reserve, 28 December 2016. [Online]. Available: https://www.federalreserve.gov/bankinforeg/regzcg.htm. [Accessed 11 Dec 2017].

[33] Force, France Financial Task.

[34] Forum, Digital Economy.

[35] P. L. 1. 2. 1. Health Insurance Portability and Accountability Act Of 1996, Health Insurance Portability and Accountability

Act Of 1996, Public Law 104–191, Washinton, DC: U.S. Federal Government, 1996.

[36] M. Brown, "Brown, Morgan. Examples of PHI, January 11, 2015," truevault.com, 11 1 2015. [Online]. Available: https://www.truevault.com/blog/protected-health-information.html. [Accessed 6 10 2017].

[37] U. D. o. Education, Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) Federal Law, Washington, DC: U.S. Department of Education.

[38] U. S. Congress, Gramm-Leach-Bliley Act, Washington, DC: 106th United States Congress, 1999.

[39] S. Haber and . W. S. Stornetta, "How to time-stamp a digital document," 1991. [Online]. Available: https://link.springer.com/article/10.1007/BF00196791.

[40] H. S. S. W. Bayer D., "Improving the Efficiency and Reliability of Digital Time-Stamping," in Sequences II, Springer, NY, 1993.

[41] V. Gupta, "A Brief History of Blockchain," 28 February 2017 . [Online]. Available: https://hbr.org/2017/02/a-brief-history-of-blockchain.

[42] R. Kotcher, "How Do Bitcoin Transactions Actually Work?," 1 June 2017. [Online]. Available: https://blockgeeks.com/bitcoin-transactions/.

[43] The Economist, "The Great Chain of Being Sure About Things," 31 October 2015. [Online]. Available: http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[44] M. Gray, "Introducing Project “Bletchly”," 16 April 2017. [Online]. Available: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md.

[45] Raconteur, "The future of blockchain in 8 charts," 27 June 2016. [Online]. Available: https://www.raconteur.net/business/the-future-of-blockchain-in-8-charts.

[46] "Improving the Efficiency and Reliability of Digital Time-Stamping," [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24.

[47] English Oxford Dictionary, "English Oxford Dictionary," Oxford University Press, 2015. [Online]. [Accessed 10 10 2017].

References

1. Adarsh, S & Ashraf, S., Chapter 2, Introduction to Blockchain Technology. Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities. Indian Institute for Information Technology and Management. 2017. pp.127.
2. Allen, A., 2011, Unpopular Privacy: What Must We Hide? Oxford: Oxford University Press.
3. Anderson, Ross. Risk and Privacy Implications of Consumer Payment Innovation. Cambridge University. https://www.cl.cam.ac.uk/~rja14/Papers/anderson-FRB-Kansas-mar27.pdf.
4. Athey, S., I. Parashkevov, S. Sarukkai, and J. Xia (2016). Bitcoin pricing, adoption, and usage: Theory and evidence. SSRN Working Paper No. 2822729, http://papers.ssrn.com/sol3/papers.cfm?abstract id=2822729.
5. Bayer D., Haber S., Stornetta W.S. (1993) Improving the Efficiency and Reliability of Digital Time-Stamping. In: Capocelli R., De Santis A., Vaccaro U. (eds) Sequences II. Springer, New York, NY. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.4891&rep=rep1&type=pdf.
6. Brown, Morgan. Examples of PHI, January 11, 2015. Retrieved from https://www.truevault.com/blog/protected-health-information.html
7. Burke, Allison. How Safe Are Blockchains? It Depends. Harvard Business Review, Technology. March 7, 2017. Retrieved 10/6/2017. Retrieved from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.
8. Cheng, Lisa. An Introduction to the Bitcoin Blockchain. January 6, 2015. Retrieved from http://insights.wired.com/profiles/blogs/the-bitcoin-blockchain-and-the-coming-tokenization-of-user#axzz4x7pZkY7p.
9. Coy, P. and Kharif, O. 2016. This Is Your Company on Blockchain. Bloomberg Businessweek. Retrieved from < http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain> on 3rd July 2017.
10. Downey, Catherine M. The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash, 14 J. Marshall J. Computer & Info. L. 303 (1996).
11. Ghosh, Rituxan. Haider, Khondoker, Kim, Pedro. Bitcoin or Ethereum? The Million Dollar Question. Johns Hopkins Carey Business School.
12. Dahan, Mariana, Casey, Michael. Blockchain Technology: Redefining Trust for a Global Economy, 06/16/2016, MIT Media Lab Digital Currency Initiative, http://blogs.worldbank.org/ic4d/blockchain-technology-redefining-trust-global-digital-economy Retrieved 8/30/2017.
13. English Oxford Dictionary. Oxford University Press. Published online: 2010. Current Online Version: 2015. Retrieved 10/10/2017.
14. Evans, David S., Interchange Fees: The Economics and Regulation of What Merchants Pay for Cards, Chapter 1, “The Economics of Interchange Fees,” CreateSpace Independent Publishing Platform (September 22, 2011), pp.226.
15. FDIC- Division of Supervision and Consumer Protection, Regulations, Risk Management Examination Manual for Credit Card Activities, XIX Merchant Processing. March 2007, pp.164-168.
16. Federal Telecommunication Standards Committee. Federal Standard, Telecommunications: Glossary of Telecommunications Terms. FS-1037C. U.S. Government. Federal Telecommunication Standards Committee, the Subcommittee to Revise FED-STD-1037B. The U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunication Sciences (NTIA/ITS), 325 Broadway, Boulder, CO 80303-3328.

Retrieved 10/31/2017. Retrieved from https://www.its.bldrdoc.gov/fs-1037/dir-032/_4768.htm.

17. Gupta, Vinya. A Brief History of Blockchain. Technology. February 28, 2017. Retrieved 10/17/2017. Retrieved from https://hbr.org/2017/02/a-brief-history-of-blockchain.
18. Haber, Stuart & Stornetta, Scott W. How to Time-Stamp A Digital Document. Revised: 26 October 1990. Journal of Cryptology. January 1991, Volume 3, Issue 2, pp 99–111.
19. Hancock M, Vaizey E. Distributed Ledger Technology: beyond block chain [Internet]. Government Office of Science; 2016. Available from: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review. Retrieved 10/31/2017.
20. He, Dong. 2016. Virtual Currencies and Beyond: Initial Considerations. IMF Discussion Notes. Retrieved 10/17/2017. Retrieved from https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf on 1st July 2017.
21. International Accounting Standards Committee. International Accounting Standards, 2000, International Accounting Standards Committee, 62 pp.
22. Jayachandran, Praveen. May 31, 2017. The Similarities of Public and Private Blockchain. IBM Blockchain Blog. Retrieved 10/6/2017. Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.
23. Kotcher, Robert. How Do Bitcoin Transactions Actually Work? June 1, 2017. Retrieved 8/10/2017. Retrieved from https://blockgeeks.com/bitcoin-transactions/.
24. Kovary, Peter & Zhou, Fangyi & Adoul, Mark. Blockchain Technical Details. Retrieved 8/10/2017. Retrieved from http://www.doc.ic.ac.uk/~ma7614/topics_website/tech.html.
25. Kroll, J., I. Davey, and E. Felten. 2013.The Economics of Bitcoin Mining, or BitCoin in the Presence of Adversaries. WEIS 2013. Retrieved from <http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf> on 1st July 2017.
26. Lee, T.B. 2014. These four charts suggest that BitCoin will stabilize in the future. Washington Post. Retrieved from <http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/03/these-four-charts-suggest-that-bitcoinwill-stabilize-in-the-future> on 1st July 2017.
27. Lewis, Anthony. A Gentle Introduction to Immutability of Blockchains. Posted on February 29, 2016, Bits on Blocks.net. Retrieved 10/6/2017. Retrieved from https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/.
28. Nakamoto, S. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System. Retrieved 8/10/2017. Retrieved from https://bitcoin.org/bitcoin.pdf.
29. Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press: Princeton NJ.
30. National Institute of Standards and Technology (NIST), NIST Special Publication 800-63, Revision 3, Digital Identity Guidelines, Appendix A—Definitions and Abbreviations. Retrieved 10/17/2017. Retrieved from https://pages.nist.gov/800-63-3/sp800-63-3.html.
31. National Institute of Standards and Technology (NIST), NIST Special Publication 800-78, Revision 4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, Retrieved 10/17/2017. Retrieved http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf
32. National Institute of Standards and Technology (NIST), NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable

Information (PII). National Institute of Standards and Technology, U.S. Department of Commerce. April 2010. Retrieved 8/1/2017. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-122/final.

33. Nicoletti, Bernardo. The Future of FinTech: Integrating Finance and Technology in Financial Services. Glossary. p. 297. Palgrave Macmillan; 1st ed. 2017 edition (March 2, 2017). Pp.328.
34. PCI Security Standards Council, Payment Card Industry Data Security Standard (PCI DSS) v3.2, PCI Security Standards Council, Retrieved 10/11/2017 from https://www.pcisecuritystandards.org /.
35. Popper, Nathanial, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money, Harper; Reprint edition (May 19, 2015), pp. 1,097.
36. Raconteur. The Future of Blockchain in 8 Charts. Raconteur, Business. June 27, 2016. Retrieved 8/10/2017. Retrieved from https://www.raconteur.net/business/the-future-of-blockchain-in-8-charts.
37. Roth, Richard. The Value of Information. Dynamic Strategic Planning. Massachusetts Institute of Technology.
38. PwC. 2015. Money is no object: Understanding the evolving cryptocurrency market. PricewaterhouseCoopers. Retrieved from < http://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf> on 1st July 2017.
39. Slawsky, Jeff, and Safar, Samee. Developing and Managing a Successful Payment Cards Business, Routledge (November 28, 2005).
40. Sorrel, Charlie. What Happens When We Become A Cashless Society? Fast Company. 03.15.16. World Changing Ideas. https://www.fastcompany.com/3056736/what-happens-when-we-become-a-cashless-society. Retrieved 6/10/2017.
41. Stallings, William. Cryptography and Network Security: Principles and Practice, 6th edition, 2014, Pearson. Pp, 758.
42. Tapscott, Don & Alex. What is Blockchain Technology? A Step-by-Step Guide for Beginners. Blockchain Revolution (2016). Retrieved from https://blockgeeks.com/guides/what-is-blockchain-technology/.
43. United States of America Federal Trade Commission Washington, D.C. 20580, Prepared Statement of The Federal Trade Commission Before the Subcommittee on Financial Institutions And Consumer Credit Committee On Banking And Financial Services on the Implications of Emerging Electronic Payment Systems on Individual Privacy. September 18, 1997.
44. van den Hoven, Jeroen, Blaauw, Martijn, Pieters, Wolter and Warnier, Martijn, "Privacy and Information Technology," The Stanford Encyclopedia of Philosophy (Spring 2016 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2016/entries/it-privacy/>.
45. Warren, Samuel D. & Louis D. Brandeis, 1890, “The Right to Privacy,” Harvard Law Review, 4(5): 193–220. [Warren and Brandeis 1890 available online]
46. World Development Indicators. Individuals using the Internet (% of the population). The World Bank, Data. International Telecommunication Union, World Telecommunication/ICT Development Report, and database. July 26, 2016. Retrieved 10/10/2017.
47. World Payments Report 2016. Capgemini. Capgemini Financial Services Analysis, 2016; Bank for International Settlements Red Book, 2014 figures released December 2015. https://www.worldpaymentsreport.com/#world-payments-report-2016. Accessed 6/10/2017.

48. Zohar, A. 2015. Bitcoin Under the Hood. Communication of the ACM. Retrieved from < http://cacm.acm.org/magazines/2015/9/191170-bitcoin/abstract> on 1st July 2017.
49. Zoldi, S. Analytic Techniques for Combating Financial Fraud. Keynote at Financial Cryptography, 2012. Kralendijk, Netherlands Antilles. February 27, 2012.

Appendix A: Glossary

Altcoin. Altcoin refers to a math-based decentralized convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One exchange, Cryptsy, reportedly exchanges over 100 different virtual currencies (as of 2 April 2014) [24].

Automated Teller Machine (ATM) Cards. ATM cards, used at automated teller machines, allow consumers to obtain cash from their deposit accounts, transfer funds, obtain account balances, and, in some cases, purchase stamps or other products [25].

Authentication. A process that grants access to a local or remote computer system, a network, or online information [26, p. 47].

Bitcoin. Bitcoin, launched in 2009, was the first decentralized convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that do not systematically link to an individual. Therefore, Bitcoin is said to be "pseudo-anonymous." Bitcoin's cap 21 million bitcoins (but each unit could divide into smaller parts). Bitcoin is projected to reach 2140.15. As of April 2, 2014, there were over 12-and-a-half million bitcoins, with a total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date (France Financial Action Task Force) [6].

Certification Authority (CA). An entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities [27, p. 18].

Credit Card. An agreement between a buyer and a seller in which the buyer receives the good or service in advance and makes payment later, often over time and usually with interest [28].

Cryptocurrency. Cryptocurrency refers to a math-based, decentralized convertible virtual currency that is protected by cryptography. —i.e., it incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another and must be cryptographically signed each time it transfers. A network of mutually distrustful parties (in Bitcoin, referred to as miners) ensure the safety, integrity, and balance of cryptocurrency ledgers. These parties protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as an incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the blockchain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods (France Financial Action Task Force [19].

A type of digital token that relies on cryptography for chaining together digital signatures of token transfers, peer-to-peer networking, and decentralization (Digital Economy Forum).

Debit Cards. Debit cards allow a consumer to authorize a merchant to electronically debit the consumer's deposit account to pay for purchases. Debit cards are widely accepted by merchants [28].

Digital Currency. Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency." The term "e-Money" may be used interchangeably with the digital currency.

Digital Signature. A coded message added to a document or data that guarantees the identity of the sender. An asymmetric key operation where the private key is used to sign data and the public key digitally is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection. [26, p. 51].

Electronic Banking. The use of a computer to retrieve and process banking data (statements, transaction details) and to initiate transactions (payments, transfers, requests for services) directly with a bank or other financial services providers remotely via a telecommunications network [25].

Electronic Commerce. The use of an information infrastructure and network communications through which businesses can exchange information, conduct customer service, manage operating costs, and support global competitiveness.

Encryption. The scrambling, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security [8, p. 658].

Electronic Money. These include stored-value cards on which cash value can stores for use by consumers at vending machines, on mass transportation systems, or other locations. Electronic money presents a wide array of consumer protection issues, including liability for unauthorized use and dispute resolution procedures [25].

Fair Credit Reporting Act (FCRA). Concerned with the privacy and accuracy of information maintained by credit bureaus [25].

Federal Trade Commission (FTC). Governing body and enforces the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices [29].

HashCode. A unique, mathematical summary or "fingerprint" of a document that serves to identify the document and its exact contents. Any change in the hash code is an alert that the document's contents have been altered.

Internet. The internet is a worldwide system of computer networks. The Internet uses a set of communication standards, known as TCP/IP, to communicate [30].

Hash Function. The process of applying a hash function to some data is called hashing. The output of a hash function is called a hash. A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. There are many types of hash functions, and a common, robust one is called SHA-256 (which stands for Secure Hash Algorithm – 256 bit) [54]. A hash function is a function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:1. One-way - It is computationally infeasible to find any input that maps to any pre-specified output; and2.Collision resistant - It is computationally infeasible to find any two distinct inputs that map to the same output [8, pp. 176-177].

Internet. a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols [25]

Kerberos. A distributed security system developed by the Massachusetts Institute of Technology. It uses private-key security [26].

m-Payment. Mobile Payment.

Personal Identifiable Information. PII, according to the U.S. Office of Management and Budget, is any information that can be used to identify, contact or locate an individual uniquely, or can be used with other sources to uniquely identify a person [5, pp. E-1].

Private-key. Security Also known as a symmetric-key security, this is a security mechanism based on both parties have the same encryption key, as in secret-key cryptography. The client and server share a key to encrypt and decrypt information on a network. A typical implementation of private-key security is the Kerberos distributed security system [26, p. 57].

Public-key Security. Also known as an asymmetric-key security or public-key encryption technology, this is a security mechanism for securely distributing encryption keys that are used to "lock" and" unlock" data across an unsecured path. Public-key security uses on encryption key pairs, in contrast to private-key security, which uses a single, shared key [26, p. 58].

Regulation E. Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account [31].

Regulation Z. The Truth in Lending Act (TILA) is implemented by the Board's Regulation Z (12 CFR Part 226). A principal purpose of TILA is to promote the informed use of consumer credit by requiring disclosures about its terms and cost. TILA also includes substantive protections [32].

RSA. An encryption mechanism by RSA Data Security that uses both a private and a public key. RSA is also used for authentication [27, p. 15].

Secure Socket Layer (SSL). A security protocol developed by the Netscape Communications Corporation to encrypt sensitive data and verify server authenticity.

Sensitive Information. Information, the loss, or misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled to under 5 U.S.C. Section 552a (the Privacy Act), but that has not been expressly authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy [25].

Truth in Lending Act (TILA). Regulation Z provides numerous protections for consumers in credit card transactions [29].

The TILA and its implementing Regulation Z provide numerous protections for consumers in credit card transactions, including a $50 limitation on consumer liability for lost or stolen credit cards and the ability for consumers to dispute charges on their bill in certain situations [29].

The Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 et seq., Truth in Lending Act ("TILA"), 15 U.S.C. § 1601 et seq., and Electronic Fund Transfer Act ("EFTA"), 15 U.S.C. § 1693 et seq. The FCRA, which is concerned with the privacy and accuracy of information maintained by credit bureaus, underwent extensive revisions last year and those amendments become effective September 30 [29].

The EFTA and its implementing Regulation E cover a variety of electronic fund transfers involving consumers, such as those with ATM and other debit cards; it does not apply to transactions that do not involve a consumer's deposit account. Under the EFTA, consumer liability for unauthorized use of a lost or stolen card is limited to between $50 and $500, depending on when the consumer reports the loss or theft [29]

Virtual Currency. A non-money based currency. Virtual currency is a digital representation of value that digitally trades. Virtual currency functions as (1) a medium of exchange, and (2) a unit of account, and/or (3) a store of value. It does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfills the above functions only by agreement within the community of users of the virtual currency. Virtual currency is different from fiat currency (a.k.a. "real currency," "real money," or "national currency"). Fiat currency is the coin and paper money of a country that it designates as its legal tender, circulates, and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to transfer value denominated in fiat currency electronically. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status (France Financial Action Task Force) [33] [19].

A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community (Digital Economy Forum) [34].

Appendix B: Examples of Sensitive Information

Table 1. Qualities of Sensitive Information

Information Type	PII	PHI	Employee Data	FERPA	Non-Public Information
Sensitive (Y/N)	**Y**	**Y**	**Y**	**Y**	**Y**
Requires Encryption (Y/N)	**Y**	**Y**	N	N	N
Applicable Security Standards (Y/N)	**Y**	**Y**	**Y**	**Y**	**Y**

Personal Identification Information (PII) Examples

Source: NIST 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) [5]

1. First or last name (if common)
2. Date of birth
3. Country, state or city of residence
4. Credit card numbers
5. Immunization history/medical records
6. Age
7. Telephone numbers
8. Email addresses
9. Gender
10. Race
11. Criminal record
12. Social security or employer Tax ID Numbers.
13. Driver’s license, State identification card, or passport numbers.
14. Checking account numbers.
15. Savings account numbers.
16. Credit card numbers.
17. Debit card numbers.
18. Personal Identification (PIN) Codes used to authorize the electronic use of a Financial Transaction Card.
19. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
20. Digital signatures (an electronic representation that is unique to an individual that is very difficult to fake since it utilizes an encryption process to ensure uniqueness).

21. Any other numbers or information that can be used to access a person's financial resources.
22. Biometric data.
23. Fingerprints.
24. Passwords.
25. Parent's legal surname prior to marriage.

Note: Electronic mail names are only considered Personal Identifying information (PII) when stored in a context that would allow access to a person's financial information or assets.

Personal Health Information (PHI) Examples

Source: Health Insurance Portability and Accountability Act Of 1996, Public Law 104–191—AUG. 21, 1996. HIPPA [35] [36]

1. Names.
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
4. All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may aggregate into a single category of age> 90.
5. Phone numbers.5. Fax numbers.
6. Electronic mail addresses.
7. Social Security numbers.
8. Medical record numbers.
9. Health plan numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plates.
13. Device identifiers and serial numbers.
14. Web Universal Resource Locators (URLs).
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or codes.

Note: These 17 identifiers are PHI when stored in combination with health information.

Typical Employee Data Examples

1. Dependent financial information.
2. Credit rating/history.
3. Non-banking related financial information.
4. Income levels, worth financial statements, and sources.
5. Work plans and fitness reports.

Family Educational Rights and Privacy Act of 1974 (FERPA) Examples

Source: Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) Federal Law [37]

1. Non-directory information (e.g. grades).
2. Student application information.
3. Student Financial Services information.
4. Wire transfer information.
5. Payment history.
6. Financial aid/grant information.
7. Student tuition bills

Non-Public Information Examples

Source: Gramm-Leach-Bliley Act [38]

1. Information covered by non-disclosure.
2. Information that if released causes reputational damage to the University.
3. Contracts.
4. Configuration details for information resources with access to restricted data,
5. Usernames and password stores,
6. Donor information.
7. Lab animal care information.
8. Copyright protected information.
9. Patent protected information.
10. Research data classified as sensitive by an IRB.

Appendix C: History and Development of Blockchain Technology

Blockchain technology appears in a Bitcoin design specification dating back to 2008 However, a key feature of blockchain dates back to the early 1990's. Stuart Haber and W. Scott Stornetta's attachment of a digital time-stamp to a document in 1990 [39]. The timestamp value is an essential aspect of the blockchain, as it helps order the blocks sequentially. Most crucially Haber and Stornetta developed a method which is both computationally feasible while also being "infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service" [39]. The second major development followed shortly after that in a paper published in 1993 by the same authors as the previous paper along with a third author named Dave Bayer. The paper is entitled "Improving the Efficiency and Reliability of Digital Time-Stamping" and describes almost exactly what the title suggests. The authors identify that the computational power needed both for verifying and storing timestamp data can be a severe limitation to their previous method [40]. To overcome this obstacle, they make use of a tree structure which reduces both the storage required as well as the computational power needed to verify time stamps and digital signatures [40]. This tree structure would go on to be called a "Merkel Tree" which, in the case bitcoin, is used to store hashes of individual transactions while the specific structure of the tree allows for rapid verification of those hashes [21]. In the case of other implementations of the blockchain, Merkel Trees can also be used to verify the integrity of whatever data that particular blockchain is being used to store.

Improvements to blockchain's technology continue, with three essential proposals over the past ten years. The blockchain technology itself has value beyond use in Bitcoin [41]. Examples include "smart contracts" or contracts that use blockchain to verify and validate a contacts life-cycle. Financial institutions use smart contracts for bonds and loans [41].

A second example uses what is known as "proof-of-stake" security. Proof-of-stake is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In Proof-of-Stake-based cryptocurrencies, the creator of the next block is chosen by various combinations of random selection and wealth or age (i.e., the stake). This model is expected to start going live late 2017 and is called "blockchain scaling" [41].

Currently, every node in the network processes each block on its own which makes for inefficient use of the computing power available for use by those nodes. With blockchain, only the number of nodes required to validate each new block does the work, which frees up other nodes to handle other blocks. This shortens the overall processing time. The speed and security of a scaled blockchain are expected to allow it to compete with transaction processors like VISA as well as break into the ever-growing internet of things [41].

Appendix D: Blockchain Execution Details

In a process called "mining," the data to be placed in a block is collected and processed. Each block can be identified by a hash and also contains the hash of the previous block in the chain [21]. This approach allows the blocks to append to the chain in the proper order. Thus, the chain of blocks can be followed all the way down to the first original block in the chain, and the longest overall chain is what is accepted by the network [21]. Updates occur only to the latest copy of the ledger.

Proof-of-work algorithms maintain a consensus of blocks in the chain across all nodes. This is known as consensus processing. Along with the data of interest, the blockchain includes an arbitrary integer called a nonce. The proof-of-work algorithms use the nonce to verify the data was processed, and not merely created by someone trying to include a falsified transaction [21]. Consensus processes help maintain the integrity of the data contained in previous blocks. If the data in one block changes, it triggers a recalculation across all blocks in the chain. Recalculation requires computing and storage resources, especially if the chain is a large chain. If the change is invalid, consensus verification fails, and the block is qualified as "corrupted." The changed or corrupted block no longer matches the consensus chain held on other nodes [21]. It may seem possible to circumvent the necessary calculations by trying to push a chain to the network that ends with the edited/falsified block. Such an attempted would be met with failure since the invalid block results in a rejection, as it is shorter than the chain on other valid nodes.

To provide an example of what a block looks like we examine the structure used by Bitcoin. In this case, an individual block (corresponding to an individual transaction) consists of three parts: the header, the input, and the output [42]. The contents of each part are as follows: [42].

Header

- Hash: The hash of this specific block/transaction
- Ver: The algorithm version to use to verify the block
- Vin_sz: The total number of inputs included in this transaction
- Lock_time: A time stamp showing the earliest time this block/transaction can be processed and added to the chain

Input

- Previous output hash: A pointer hash showing valid available spend
- N: An index showing the actual amount being spent by the sender

- scriptSig: A script showing the spender has permission to send the currency referenced by the first two input fields.

Output

- value: The number of bitcoins to spend (expressed in the unit “Satoshi” which is equivalent to 1/100,000,000th of a single bitcoin)
- scriptPubKey: This is the other script provided in each bitcoin transaction which points to a hash of the public key owned by the recipient of the bitcoin. This mostly makes up the address of the recipient.

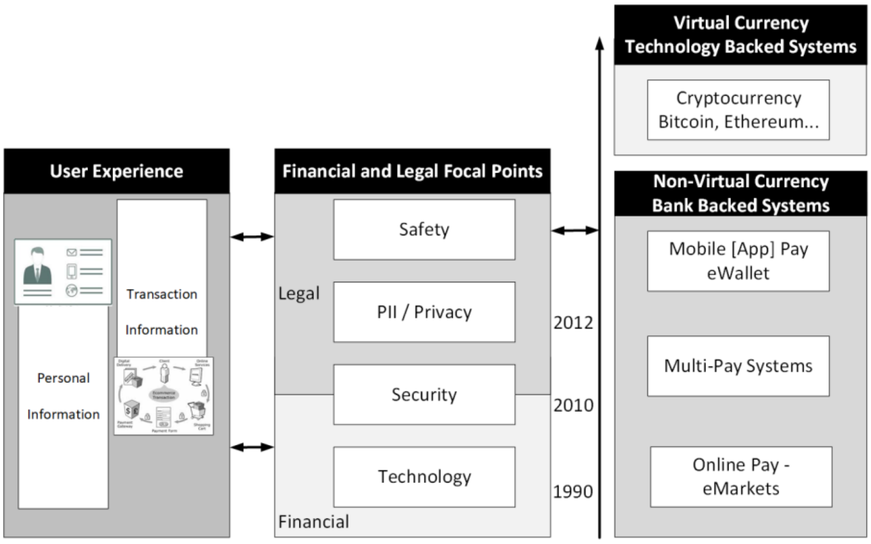
Before the block addends the chain, it must be qualified as a valid transaction. This is accomplished using the two scripts each found in the input and output. The first script (scriptSig) proves the spender can spend the bitcoin they claim they can while the second script (scriptPubKey) verifies the recipient is who say they are by checking the public key provided by the recipient against the hash provided by scriptPubKey [42]. If both scripts return true, then the transaction is valid, executed, and added to the blockchain.

If two blocks process in a short enough time interval that they both contain the hash for the same block in the chain, then the chain is “forked” [21]. Both blocks add to the chain at the same position, and the chain overall can remain valid (as long as it maintains consensus with the chains held by other nodes. New blocks can add to either fork; however, in the course of time, one fork becomes longer than the other. This longer fork becomes the preferred branch for the addition of new blocks by the network [21]. The shorter fork remains present in the chain to maintain the integrity of the data contained within those blocks but is ignored by the network regarding the addition of new data (though it is possible for that short fork to become preferred if it does somehow become longer than the other fork).

Appendix E: Evolution of Electronic Payments

Fig. 17 is a model depicting types of information enmeshed in a user experience, focal points of both legal and financial standards and practices, and an evolutionary timeline to cashless transactions. ***User Experience*** consists of the information at the center of a user experience: Personal Information and Transaction Information, or information needed to initiate and complete an exchange.

The focus ***of U.S. practices and standards*** is around safety, the protection of personal information or privacy, security, and technology. Fundamental policy and legislation ensure personal information is kept safe and secure, and that systems which utilize and produce information about a transaction meet specific technical operating requirements to protect and secure information during use and storage.

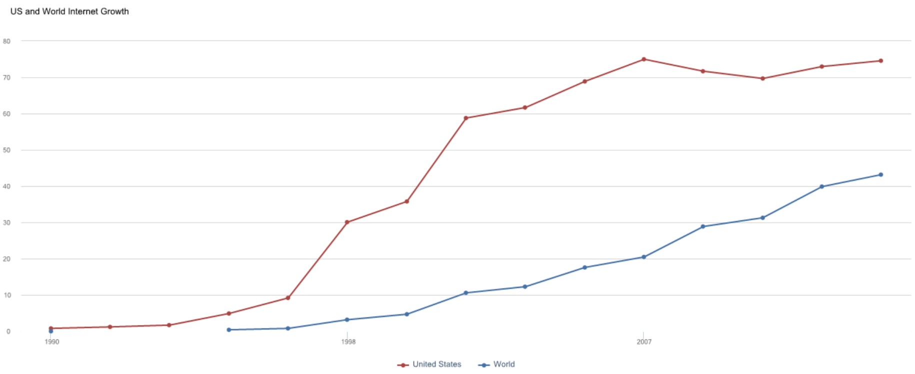


Virtual Currency: Not always backed by Physical Assets; **Does NOT have a Legal Tender Status**
Non-Virtual Currency: Backed by Physical Assets: **Does have a Legal tender Status**

Fig. 17. Critical Components of a Cashless Transaction

Finally, the evolution from cash-based to cashless transactions accelerated in the early 1990’s with the onset of online payment methods (Amazon Online markets, Barnes and Noble's online market, eBay Stores). Payment systems quickly advanced to multi-payment systems such as PayPal, Apple Pay, Android Pay, Google Pay and finally to more current mobile payment systems like Apple Wallet, Bit Wallet, Google Wallet and so forth. These pay systems are still ***currency-based exchange systems***, using a currency backed by physical assets managed by centralized U.S. banking system, and recognized worldwide. Within the last seven years, a ***virtual currency*** or technology generated cryptocurrency (Bitcoin, Ethereum) has emerged as alternative currency source. While not considered mainstream (i.e., not backed by physical assets managed by a centralized banking system), cryptocurrency has introduced a transaction registration technology called “blockchain” that has the potential to disrupt how transactions are recorded and controlled.

Exponential Growth of the Use of the Internet, World and United States



1990-2016
Time : 1992,Series : Individuals using the Internet (% of population)
Source: World Development Indicators
Created on: 10/31/2017

Fig. 18. United States Individuals Using the Internet (% of Population) 1990-2010. 76.17 % of the United States' individuals use the internet. 45.91 % of the World's individuals use the internet. Source: The World Bank Data. Retrieved October 31, 2017.