SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER

Blockchain and Smart Card Technology

Version 1.0

Date: March 2017

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Table of Contents

1 Introduction

Blockchain technology, the potentially revolutionary technology that implements bitcoin transactions, is suitable for use in a wide variety of applications. Both startups and established players are deploying or piloting blockchain applications; over $1 billion has been invested in blockchain and bitcoin startups since 2009, with 60 percent of that funding occurring since the beginning of 2015.[1]

A blockchain is a distributed database that maintains a dynamic list of records, secured against tampering and revision.[2] Blockchains can be used as distributed ledgers that allow financial (and other) transactions to be recorded and verified cryptographically without the requirement for a central clearinghouse or authority.

This white paper was developed by the Secure Technology Alliance Payments Council to stimulate industry discussion on innovative blockchain applications. The white paper provides a primer on blockchain technology, including the role of the secure element and of smart card technology in securing transactions. It describes use cases that are currently commercially available or being piloted and discusses common implementation considerations.

[1] CB Insights webinar, "The State of Blockchain," https://www.cbinsights.com/research-blockchain-transcript.
[2] Wikipedia, https://en.wikipedia.org/wiki/Block_chain_(database).

2 Bitcoin and Blockchain Technology

The concept of bitcoins, or electronic cash, was born from the idea that an ownerless, open-source, transparent, and decentralized currency backed by cryptography could represent a dramatic improvement over government-backed currencies. The idea was pioneered by a group of mathematically minded individuals who were concerned about loss of privacy and institutional overreach by banks and governments. Designing such a digital cash system faced several technical challenges. One is the double-spending problem: unlike physical token money, electronic files can be duplicated, and hence the act of spending a digital coin does not remove its data from the ownership of the original holder. Most experimental currencies solved this by relying on a central authority, which represented a single point of vulnerability and the potential for abuse. Removing this central authority and relying on a pure decentralized network then poses the problem of Sybil attacks, where one entity tries to gain a disproportionately large influence on the network.

In 2008, the pseudonymous developer Satoshi Nakamoto published a white paper[1] describing a cryptocurrency – Bitcoin – relying on a purely distributed ledger with safeguards to prevent both double-spending and Sybil attacks. One of the guiding principles of Bitcoin is that, like the gold standard, the currency is not subject to debasement or value manipulation by central banks.

The Bitcoin payment technology relies on a more general technology called blockchain technology. It implements a ledger, used to record the ownership of each bitcoin. This ledger is shared among all computers on the Bitcoin payment network, and each transaction is validated using a cryptographic puzzle. The puzzle is a computationally intensive hash algorithm: find a *nonce*—a random number—such that the hash of the transactions and the nonce has a correct number of leading zeros. The first computer to solve the puzzle, verifying and approving the transaction, is paid with newly created bitcoins (the individual running the computer is called a *miner*; the process is referred to as mining). Then, if a majority of the other computers on the network agree with the solution, the transaction is entered on the blockchain. The network is referred to as a consensus network, and it enables a new payment system and a new form of digital money, also known as cryptocurrency.

The Bitcoin network has far more computing power than the 500 fastest supercomputers in the world. It constitutes a crowd-owned, public, transparent, and safe transaction system, impervious to attack. It represents the first decentralized, user-driven, peer-to-peer payment network functioning without a central authority. Each transaction is identified by a unique number. Once the transaction is entered into the ledger, the bitcoin that was spent in the transaction cannot be used again. A slightly decreasing number of new bitcoins are generated daily, leveling off in 2140 at 21 million.

Although the bitcoin payment network has been subject to speculation, association with criminal activity, and hacking, the technology is still evolving. Average daily transaction volume for bitcoins has already surpassed that of Western Union,[3] although Visa transaction volume is still 60 times larger.

[3] Coinometrics, "How Bitcoin Activity Stacks Up Against Other Payment Networks," https://d28wbuch0jlv7v.cloudfront.net/images/infografik/normal/ChartOfTheDay_1681_Daily_transaction_volume_of_payment_networks_n.jpg.

2.1 Technology Overview

Bitcoins are analogous to the rai stones on the Island of Yap.[4] Rai stones are huge limestone discs, up to 12 feet across and weighing up to 4 tons, that were used as money on the Pacific Island of Yap as early as 1000 AD and until the late 19th century. The stones were so large that it was impractical to move them, so people kept track of who owned each one through oral history. The ownership history of each stone was documented through this shared oral ledger; the stones themselves never changed hands. Blockchain technology can be viewed as the digital version of this oral ledger. It enables the maintenance of a distributed database that constitutes a virtual ledger shared by multiple participants.[5]

2.1.1 Basic Principles

Blockchain technology relies on the following basic principles:

1. Decentralization. There is no central authority, with no single point of vulnerability or failure.
2. Trustlessness. A blockchain does not require trust in any authority or any participant.
3. Consensus network. A process allows participants to come to an agreement over what is true or false. For a cryptocurrency, it would typically concern the validity of a transaction.
4. Transaction transparency. The validity of all transactions is available to everyone on the network.
5. Transaction immutability. Once added to the blockchain, a transaction cannot be changed or manipulated.
6. Pseudonymous. Transactions are anonymous (in that they do not require personal information) but can be traced back to a public key.

2.1.2 Description

As already stated, a blockchain is a shared, trusted public ledger that everyone can inspect, but which no single user controls. Participants collectively keep the ledger up to date; it can be amended only according to strict rules and by general agreement. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

In any blockchain-based service, two families of actors can be identified. On one hand, the "users" are the ones using the service by producing transactions, for instance exchanging money one with one another.[6] They use standard cryptographic techniques to prove that they are legitimate to instantiate a specific transaction. For example, in Bitcoin, if a transaction stored in the ledger states that Bob has given 3 bitcoins to Alice, someone willing to spend these 3 bitcoins must prove she is Alice. Actually, "Bob" and "Alice" are replaced by public keys, so proving a user is Alice is done by providing a signature with the corresponding private key. When a user has produced a transaction, the transaction is sent to the second actor of the blockchain: the blockchain network.

---

[4] Stetson University, Master of Accountancy (online) course, http://www.stetson.edu/online/macc/bitcoin-definition-and-analysis-infographic/.

[5] Wikipedia, https://en.wikipedia.org/wiki/Block_chain_(database).

[6] It is important to note that a blockchain application may support anonymous or pseudonymous users (as with Bitcoin) or the application may have a separate process for establishing a user's identity prior to producing a blockchain transaction. A "user" may be a person or non-person entity. Discussion of establishing user identity is not covered in this white paper.

The network is (usually) a peer-to-peer network formed of nodes that receive the transactions. The nodes are in charge of checking the validity of the transactions; this means that each node checks the signature of the transactions it receives with respect to the version of the history it is aware of. Remember there is no central authority, hence no trusted copy of the ledger. Once a node has checked enough transactions, it makes a "block." A block is a batch of validated transactions that must comply with different requirements: it includes a reference to the last block the node knows (typically, a hash of this block), a timestamp, and the "proof." (Figure 1) The proof is the piece of data required by the consensus algorithm. This algorithm allows nodes to agree on the right version of the ledger even though there is no reference version.

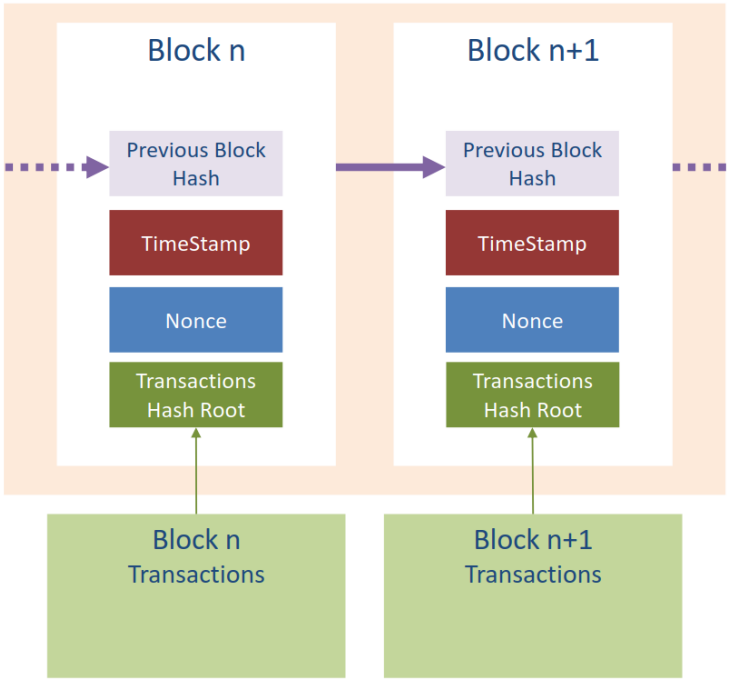

Figure 1. Creation of a Block

The consensus algorithm is the core aspect of the blockchain. Several techniques exist. The Bitcoin blockchain, for example, uses a proof-of-work based consensus: in order to produce a valid block, a node has to solve a computationally difficult task. More specifically, it has to find a *nonce*—a random number—such that the hash of the block has a correct number of leading zeros, defined by the algorithm. The nonce is the proof to be included in the block. Once a node has managed to produce such a block, it broadcasts it to the other nodes of the network. The other nodes then perform the following checks: check the validity of every transaction embedded in the block with respect to its local version of the history, check that the referenced previous block exists and is valid, check the timestamp is greater than the one of the previous block, and check that the proof is correct. If the block is judged valid, then nodes append it to their version of the ledger, and start working on the next block.

Obviously, as there is no unique, central copy of the blockchain, several versions of it exist in the network at the same time. These different versions are called "forks." (Figure 2) The rule for each node is to work on the longest valid chain it is aware of. By doing so, some forks are abandoned and only one of them eventually "wins." Indeed, if a majority of CPU power behaves according to the rule, the chain that will grow the fastest is an "honest" chain. Imagine an attacker willing to "rewrite the history," for example removing the transaction where the attacker gave money to buy a car, after the car is

delivered. This attacker would have to go against all the honest nodes and still produce a longer chain. As changing a block changes its hash and hence breaks the chain, this attacker must invest huge computing power – in the case of a proof-of-work – especially when several blocks have been appended to the one he wants to change. When enough blocks have been appended, an attacker must surpass the power of all other nodes, and this is considered to be impossible. This is why in Bitcoin, one has to wait approximately one hour for a transaction to be sufficiently "confirmed:" this is the time needed for computing six blocks forward.[7]

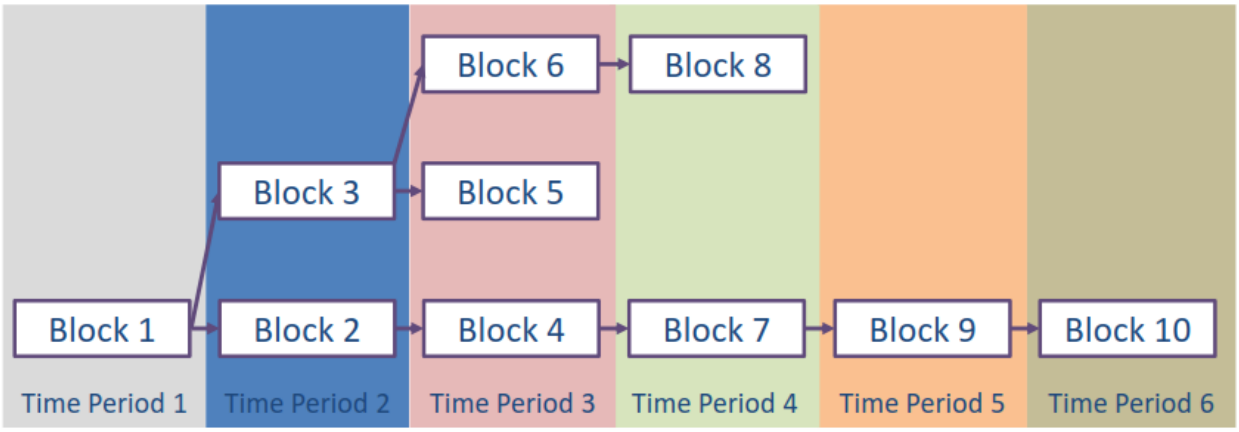

Figure 2. Blockchain Forks

2.1.3 Terms and Definitions

The following terms are used in discussions of blockchain technology.

- *51% attack*. In a proof of work based consensus, a situation in which more than half of the computing power on a blockchain network is controlled by a single participant or group of participants. This situation gives the individual or group control over the network, including the ability to stop someone else's transaction. See *consensus network*.
- *Altcoins*. Cryptocurrencies that are not bitcoins.
- *Consensus network*. A network where the blockchain is updated according to a consensus among the miners. The consensus is implemented with an algorithm that can be based on different types of proofs: proof of work, proof of stake.
- *Digital/bitcoin address*. An address from which bitcoins (or transactions) can be sent and where they can be received. A digital/bitcoin address is equivalent to *public key*.
- *Cryptographic hash*. A mathematical process that maps a variable amount of data to a shorter, fixed-length output. A hashing function has two important characteristics. First, it is mathematically difficult to work out what the original input was by looking at the output. Second, changing any of the input will produce an unpredictable and entirely different output.[8]
- *Hash rate*. The number of hashes all *miners* in a network can perform in a given period of time.

[7] https://en.bitcoin.it/wiki/Confirmation
[8] Coindesk, "Bitcoin Glossary," http://www.coindesk.com/information/bitcoin-glossary/.

- *Miner*. An individual who runs a computer system that repeatedly calculates hashes to create a successful block and earn bitcoins, both from transaction fees and from the creation of new coins with the new block. The analogy is to gold miners who discover gold that can be used to create new coins; a similar kind of discovery occurs when a successful hash creates new bitcoins.
- *Permissioned network*. A distributed network in which each endpoint is an authorized party. When the copy of the ledger can be used only by the authorized parties, it is a permissioned private blockchain. If the copy is available to everyone but the ledger update is still handled only by authorized parties, it is a permissioned public blockchain.
- *Permissionless network*. A distributed network in which the validity of a transaction is enforced by a consensus algorithm, such as *proof of work* as used with bitcoin. Early blockchain implementations are permissionless networks. Permissionless networks are also referred to as *public networks.*
- *Private key***.** An alphanumeric string forming the private part of a key pair. It is known only to the key's owner and is used to produce the signature for digital communications.
- *Public key*. An alphanumeric string forming the public part of a key pair. It is publicly available, and used to verify the signature for digital communications. In bitcoin, an address is a representative of the public key.
- *Proof of stake*. A type of proof for a consensus algorithm, where miners must prove ownership in a particular amount of currency in order to produce valid blocks. Proofs of stake are less power consuming and potentially more efficient than proofs of work by eliminating the need for computationally intensive hash algorithms.
- *Proof of work*. A type of proof for a consensus algorithm, where miners have to solve a computationally expensive puzzle in order to produce valid blocks. Typically proof of work is a result of applying a computationally intensive hash algorithm that solves for a nonce. The hashed data is proof of work.

2.2 Smart Card Technology and Blockchain Applications

Many use cases and applications are now being developed that use blockchain technology, with several recent implementations and use cases described in Section 3. All implementations of blockchain-based applications have the common security requirements of generating, storing and managing the user's cryptographic keys and would benefit from convenient user access and use of their keys.

The smart card chip or embedded secure element contains a secure microprocessor, RAM, nonvolatile memory, and (typically) a crypto-coprocessor. The memory and processors are protected physically, using a variety of software and hardware security technologies. Implementing blockchain applications using smart card and secure element technology brings the following benefits:

- Generates and protects user cryptographic keys. Smart card and secure element technology is purpose-built to perform key pair generation and other cryptographic operations quickly, with low power consumption. Because a hardware-based secure element is used, key pair generation is performed securely and is efficiently protected, even from advanced attacks. Smart card and secure element technology protects private keys in hardware with tamper-resistant hardware security and interaction restricted to a limited set of commands and responses.

- Provides straightforward user access to cryptographic keys. Smart card and secure element technology enables multiple form factors (e.g., card, USB devices, mobile device secure element, microSD, embedded secure element chip, wearables). This provides convenient, portable, user-controlled access to the keys used for blockchain transactions.
- Provides blockchain application implementers with a standards-based security platform and established standardized security evaluation and certification programs (e.g., Common Criteria).

Examples of the use of smart card and secure element technology in blockchain applications are included in the vault (Section 3.1) and NFC front-end (Section 3.2) use cases. The blockchain use cases for funds transfer, asset tracking, asset registry and the Internet of Things (IoT) described in Section 3 would also benefit from using smart card and secure element technology for convenient key generation, access and management.

3 Blockchain Technology Implementations[9]

This section describes several blockchain technology implementations including value propositions, implementation considerations and real world examples.

Included are the following use cases and critical infrastructure functions for blockchain applications:

- Cryptocurrencies
- Vaults
- Communications front end (NFC or QR code)
- Interbank funds transfer
- Asset registry
- Anticounterfeiting
- Internet of Things (IoT)

3.1 Cryptocurrency

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
A digital currency in which cryptographic techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central authority	Pseudonymous No central authority Accessible globally No chargebacks Security Low transaction fees	Exchanges Mining hardware ATMs Wallets Payment processors Merchants Handset manufacturers Internet providers Consumers, other users	Volatility and risk of loss Irrevocability Regulatory issues Negative public perception	Bitcoin Litecoin Ripple XRP Peercoin

Cryptocurrencies are digital currencies that rely on cryptographic technology to regulate generation of the currency and verification of transactions. The first cryptocurrency to be created was Bitcoin, in 2009. More than 669 cryptocurrencies (or altcoins) were available for trade in online markets as of August 24, 2015.[10]

Like gold and silver, cryptocurrency derives its value from supply and demand. Value is not controlled by any country, central bank, or other single authority. A cryptocurrency has no physical form; the network generating the cryptocurrency is completely decentralized, with all transactions performed only by the system users. Transactions are irreversible and generally pseudonymous—that is, the transactions are linked to a consumer's public key, not to an individual. The transactions use cryptography for security and anticounterfeiting measures.

Cryptocurrencies are based on the concept of money as information: the money is a string of bits, sent as a message.

[9] Company, product and service references are included with the examples to document the use cases. This white paper does not endorse any specific company, product or service.

[10] Wikipedia, List of cryptocurrencies, https://en.wikipedia.org/wiki/List_of_cryptocurrencies.

Cryptocurrencies maintain a publicly visible distributed ledger that is shared across a computing network. This means that every transaction is accessible and can be inspected. Note however that, because consumers perform transactions using public and private keys, their identity is not disclosed in the distributed network and not available in the ledger. A cryptocurrency transaction typically proceeds as follows.

1. Alice wants to give Bob cryptocurrency.
2. The cryptocurrency is transmitted in the form of a message—for example, "I, Alice, am giving cryptocurrency with the public key 123456 to Bob."
3. Alice attaches her unique code to this message. The code is actually a digital signature.
4. The cryptocurrency is sent to the network and information that Bob owns the cryptocurrency is logged in the public ledger.
5. The nodes on the network agree to the transaction.

In traditional cross-border remittances, the appropriate banking and clearing systems complete a transaction, which requires time for settlement and incurs transaction fees. Cryptocurrency transactions can send money to parties on the network more quickly than traditional transactions. Cryptocurrency transactions do not incur fees for cross-border or international money transactions. Cryptocurrencies can be sent to any person in the world within minutes, making the transaction look like a real-time transaction. Cryptocurrency transactions are currently not governed by any regulations, although banks and other payment industry players are testing the cryptocurrency blockchain potential.

Cryptocurrency security relies on cryptography and consensus algorithms, making them impervious to counterfeiting and irreversible (no chargebacks).

There are several cryptocurrencies available in the market; examples include the following:

- In April 2011, Namecoin, the first altcoin, uses proof-of-work algorithm to store data within its own blockchain transaction database.
- In October 2011, Litecoin became the first successful cryptocurrency to use scrypt as its hash function, rather than SHA-256.
- Ripplecoin, created in 2011, was built on the same protocol as bitcoin but serves as a payment system only—a Paypal for cryptocurrencies that supports any currency, cryptocurrency, commodity, or even frequent flier miles.

3.1.1 Implementation Considerations and Challenges

While the use of a cryptocurrency provides money transactions with privacy and security, there are still challenges for cryptocurrencies and cryptocurrency service providers.

One issue is trust. Consumers must feel safe in the knowledge that the cryptocurrency will not be stolen or lost, if the cryptocurrency exchange which allows consumers to trade cryptocurrency disappears. Several bitcoin exchanges (such as Mt.Gox, BitInstant, and Flexcoin) have been subject to security breaches in which bitcoins were stolen and the exchange collapsed, resulting in losses for consumers.

Another important challenge is when and how cryptocurrency service providers will be regulated. There is currently no central authority to govern cryptocurrencies; many countries have regulations preventing the acceptance of cryptocurrency payments.

An additional consideration is volatility. Cryptocurrency value fluctuates depending on demand and supply. The value of the cryptocurrency in the distributed ledger system is purely dependent on consumer usage.

One final issue is risk of loss. Spending coins requires providing signatures with the right key. However cryptographic keys can be lost through malicious attacks, hard disk crashes, software malfunction, and consumer sloppiness. This results in the loss of the Bitcoin attached to these keys. The use of hardware-based wallets or vaults, or storage of physical copies of the cryptographic keys, are required to reduce this risk of loss.

3.1.2 Real World Examples

Digital payment methods have been becoming more popular over time, and payments using cryptocurrency are increasing. Cryptocurrencies such as bitcoin, Litecoin, and Peercoin have been successful.

Many cryptocurrency exchanges use blockchain technology for money transactions, handling smart contracts, handling smart properties, or notary services. Two examples are Ethereum and DigitalNoteXDN.

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference. The apps run on a custom blockchain that can move value around and represent the ownership of property.

DigitalNote XDN is a cryptocurrency based on the CryptoNote anonymous technology, updated with a unique, untraceable encrypted messaging system and blockchain-based deposits. Nobody owns or controls DigitalNote. It uses a proof-of-work mining process to operate without any central authority.

3.2 Cryptocurrency Vault

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Secured storage for multiple cryptocurrencies that can provide additional security layers for accessing the cryptocurrency Cryptocurrencies are stored securely online	Secure, safe funds storage Offline processes for signing transactions Privacy	Vault device manufacturers Consumers, other users Exchanges Handset manufacturers Internet providers Vault storage systems Microprocessors and interfaces Email providers	Time delayed withdrawals Multiple approvers Offline storage Multiple storage vault locations	Coinbase Xapo DNotes Ledger BTChip HW.1

Cryptocurrencies are protected by secret cryptographic keys. Whoever knows those keys can instantly and anonymously move the funds by spending them. This makes theft of cryptocurrency private keys attractive to attackers, who have been able to steal cryptocurrency worth millions of dollars. Even

major bitcoin companies can fall prey to such attacks; for example, the Mt. Gox[11] bitcoin exchange lost $450 million.

Cryptocurrency exchanges should be able to manage private keys correctly and protect consumers from both accidental loss and theft. Several methods of key management have been tried; each method is vulnerable to some extent. A common approach to storing cryptocurrency is cold storage, in which the consumer's cryptographic keys are stored on a device that is not connected to the Internet. The keys are stored in a *vault*.

A vault is digital, secured storage that can store multiple cryptocurrencies. The vault can be treated like a savings account, providing for withdrawals using various verification methods. Once authenticated, consumers can use their private keys to sign cryptocurrency transactions or conduct payment transactions using the cryptocurrency payment infrastructure.

A vault may be implemented as a cloud-based service or with a user-controlled hardware device (e.g., a smart card or USB device). A vault implemented using a user-controlled device with a secure element (SE) is considered more secure because it is not connected to the Internet. It can also come with a security certification by a third party (e.g., Common Criteria), which prevents having to trust an online service.

Additionally, a cryptocurrency vault can be stored at multiple safe locations disconnected from the Internet. That way, if one vault is compromised, another vault has a record of the data. Online vaults are typically protected using biometric scanner access, 24 x 7 video surveillance, and armed guards.

Vaults not only protect cryptocurrencies against malicious theft, they also help consumers who accidentally misplace their private keys. When consumers lose their private keys, coins become irretrievable forever. Consumers can lose their keys either through a hard drive crash or a software malfunction. The simplest solution to this problem is for consumers to print their private keys (or to use a seed to recover all of them, as proposed by the Bitcoin standard BIP 0032) and store the hard copy somewhere safe.

3.2.1 Implementation Considerations and Challenges

Important considerations are whether the vault is implemented as an online service or as a separate user-controlled hardware device and how the data is secured.

Cryptocurrency private keys can be stored in hardware vaults which use smart card technology. This may be a smart card, USB device, wearable or other mobile device. This implementation stores consumer cryptographic keys in a security domain with no access to the Internet. The vault communicates with the network via a mobile device or a personal computer, and transactions are produced without exposing the secret keys outside the vault. The hardware vault system is designed to be immune to computer viruses that steal from software wallets.

Vaults store cryptocurrency with different security features (e.g., time delays, multiple approvers). For example, the Coinbase Vault stores a consumer's cryptographic currency using the Coinbase Wallet or the consumer's Coinbase account. The consumer's cryptocurrency keys are stored in the vault (online account); the same ledger information is stored in offline vault cold storage as well. Consumers can retrieve cryptocurrency directly from vaults to their Coinbase account using an authentication process.

[11] Wikipedia, Mt. Gox, https://en.wikipedia.org/wiki/Mt._Gox.

Using vaults involves certain challenges. For one thing, withdrawals are not immediate when an online service is used. Consumers may need to wait 48 hours before the cryptocurrency is withdrawn from the vault (the length of the delay can vary based on the vault's authentication procedures). The delay can be longer if the process for initiating a withdrawal involves multiple approvers.

An additional challenge results from the need to restore consumer keys in case of data theft or loss. The online vault may therefore be located in multiple geographic locations to ensure that the information is available if one of the vaults is compromised. Vault storage at multiple geographic locations requires additional infrastructure.

Lastly, there are emerging industry-wide standards for vault implementations for Bitcoin.[12] Vault system providers are coming up with additional layers of security to safeguard consumer cryptocurrency.

3.2.2 Real World Examples

Different vaults leverage blockchain technology in different ways.

3.2.2.1 XAPO

In 2015, Xapo launched an online bitcoin vault to provide security for consumers to acquire, use, and manage bitcoins. The Xapo vault uses cryptographic security, multifactor authentication, and private key segmentation to safeguard bitcoins. Xapo vaults are located in multiple locations, providing for ledger recovery in case of a data loss.

3.2.2.2 DNOTES VAULT

In 2014, DNotes developed the DNotes vault for receiving, sending, and storing DNotes cryptocurrency. The DNotes vault stores the DNotes cryptocurrency online; the cryptographic keys are kept in cold storage in different geographic locations. The consumer can store the DNotes currency in the vault and needs to use two-factor authentication before initiating the withdrawal request.

3.2.2.3 LEDGER HARDWARE VAULT/WALLET

In 2015, Ledger developed Ledger Nano, a USB hardware vault that integrates an SE and the Ledger Operating System. The Ledger Nano connects to a computer through the USB port and stores received bitcoin information in the SE.

3.2.2.4 BTCHIP HW.1

In 2014, BTChip HW developed BTChip HW.1, a hardware wallet/vault to store bitcoin-based cryptocurrency assets safely. HW.1 connects to a computer using USB protocols and stores the cryptographic keys in the SE. The device comes with an Auto Wipe feature that erases the stored cryptographic keys after three unsuccessful attempts during device authentication via PIN.

3.2.2.5 MYCELIUM CARD

In 2016, Mycelium introduced the Mycelium card to perform regular fiat payment transactions using blockchain technology. The Mycelium card uses the colored coins protocol as implemented by Colu (blockchain based technology provider), in which the data storage mechanism is fully decentralized. The Mycelium card is a battery-powered card that includes an SE with a keypad and a display. The user sets up the authentication keys and loads the card with bitcoins using the Mycelium wallet.

[12] See, for example, BIP 32, BIP 38, BIP 44 at https://github.com/bitcoin/bips.

A payment transaction is initiated using Mycelium (on a smartphone, tablet, or Web browser), and an invoice number is generated. The user receives the invoice number. To initiate payment, the user keys the invoice number in to the Mycelium card. When the card locates the referenced invoice in the back-end system, it displays item details and the amount to be paid in fiat currency. Once authentication is achieved using keys entered by the user, the payment transaction is completed on the card, and the transaction is stored in flash memory on the card. Payment transactions are moved from the card to a blockchain (ledger) as soon as the card comes in proximity to Mycelium hub (a channel that communicates with the blockchain). Once the transaction is written to the ledger, it is removed from the card's flash memory.

3.3 Communications Front-End for NFC to Replace QR Codes

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Use of NFC as a mechanism for accessing cryptocurrency	More reliable and secure than QR codes	ATMs Mobile wallets Payment processors Merchants Handset/POS manufacturers Consumers, other users	Acceptance Volatility	Plutus Bitcoin Wallet Dangerous Things BitPlastic Coinkite Cryptopay

Most early implementations of cryptocurrency and bitcoin wallets rely on the use of QR codes to communicate the receiver's public key to the sender. While this implementation is simple, it is less reliable than Near Field Communication (NFC). How readable a QR code is depends on factors such as lighting, viewing angle, and clarity of the image. For this reason, some apps are starting to use NFC as the communications front end for mobile wallet apps. Moving to NFC expands the potential for future use cases to include wearables, where the use of QR codes is more problematic.

3.3.1 Implementation Considerations and Challenges

Implementation works similar to today's contactless transactions, with the added complexity of having to accept a new currency, potentially over a new payment network.

For person-to-person transactions, each person needs a mobile cryptocurrency wallet on a phone supporting NFC. All participants have to provision their wallets by buying bitcoins or other currency.

For proximity payment to a merchant, a wallet like Plutus (Section 3.3.2.4) can be used. The transaction goes over the traditional contactless payment network by first converting bitcoins into fiat currency. The only requirement is for the merchant to accept contactless payments.

To pay a merchant with actual bitcoins requires that the merchant be set up to accept bitcoins. Coinbase and BitPay act as the bitcoin acquirers for most of the mainstream bitcoin-accepting merchants and payment service providers (PSPs).[13] Alternatively, merchants can set up their own

[13] Chris Dickey, "Current State of Bitcoin Acceptance," First Annapolis Consulting Services, November 2014, http://www.firstannapolis.com/articles/current-state-of-bitcoin-acceptance?status=success.

cryptocurrency wallet (as in the person-to-person use case) and use a phone or tablet instead of a traditional POS terminal to process payment.

Many of the challenges are quite similar to the challenges faced by traditional contactless payments, including acceptance, availability of hardware, integration with EMV technology, and clerk training. Other challenges, such as volatility, are associated with accepting cryptocurrency. To neutralize the volatility of bitcoins, Coinbase and BitPay allow merchants to convert bitcoins immediately into U.S. dollars or other fiat currency.

3.3.2 Real World Examples

Implementation can take a variety of forms.

3.3.2.1 BITCOIN WALLET

The bitcoin mobile wallet app for Android and Blackberry works with both NFC and QR codes, allowing a person to transfer coins to someone else's phone.

3.3.2.2 DANGEROUS THINGS

Taking the concept of wearables to an entirely new level, Dutch native Martijn Wismeijer, also known as "Mr. Bitcoin," injected two NFC chips into the backs of his hands and used NXP Tagwriter to store private keys secured with BIP-38 encryption onto the devices.[14] The NFC chips are sold by Dangerous Things.

3.3.2.3 BITCOIN DEBIT CARDS: BITPLASTIC, COINKITE, CRYPTOPAY

Several bitcoin debit cards are secured using EMV contact or contactless technology. Three prime examples are BitPlastic, Coinkite, and Cryptopay. They are marketed as mechanisms for anonymously withdrawing funds and shopping. To be interoperable with the card networks, banks issue the debit cards branded as Visa or Mastercard cards. Because the card users are anonymous, the cards are subject to fairly low load limits in order to comply with appropriate regulations.

3.3.2.4 PLUTUS

Plutus uses a blockchain to convert digital currency to fiat currency before charging it to a prepaid virtual debit card secured inside the app and accessible over NFC at stores worldwide with contactless payment terminals.

By connecting bitcoin and blockchain technology with the global contactless payment infrastructure, Plutus has developed a proof of concept for performing POS transactions using NFC and paying with bitcoins.

Plutus[15] is a mobile application that allows consumers to tap and pay, using bitcoins, at any NFC terminal that accepts fiat currency (currency established as money by government regulation or law). Plutus uses the Plutus DEX platform to convert bitcoins into contactless NFC payments without a centralized exchange. The Plutus DEX platform is a decentralized peer-to-peer exchange network that uses smart contracts running on the Ethereum blockchain to handle digital currency trading.[16]

---

[14] Grace Caffyn, "Meet the Tiny Bitcoin Wallet that Lives Under Your Skin," CoinDesk, Nov. 11, 2014, http://www.coindesk.com/meet-tiny-bitcoin-wallet-lives-skin/.

[15] Plutus, "Case Study," https://plutus.it/case-study.

[16] Ethereum/wiki, "White Paper," https://github.com/ethereum/wiki/wiki/White-Paper.

An NFC payment transaction using bitcoin and Plutus works as follows:

1. The consumer signs up for Plutus and deposits bitcoins.
2. Smart contracts forward the bitcoins to the trader on Plutus DEX.
3. The trader's fiat deposit is released from escrow (Plutus Bank) into the consumer's tap and pay balance. The result is a true peer-to-peer exchange network on the blockchain.
4. The smart contract automatically notifies the DEX database to fund the consumer's virtual debit card with an equivalent amount in local fiat currency.
5. The consumer uses the debit card to tap and pay with an NFC-compliant mobile device.
6. The merchant receives payment in the form of fiat currency directly from the virtual credit card funded by the trader who received the consumer's bitcoins.

3.3.2.5 SHIFT CARD

Very few merchants accept cryptocurrency as payment, making it difficult for consumers to make regular purchases using cryptocurrency. The Shift Card is a Visa debit card that currently allows Coinbase users in 24 U.S. states and territories to spend bitcoins anywhere Visa is accepted. Shift cardholders can therefore spend bitcoins at over 38 million merchants worldwide.

Coinbase is a bitcoin exchange company. The Coinbase wallet allows Coinbase consumers to store bitcoins; consumers can use Coinbase to exchange bitcoins into fiat currencies. Consumers with a Coinbase account who want a Shift Card must apply for the card, incurring a minimal fee.

A payment transaction using the Shift Card works as follows:

1. A consumer swipes a Shift Card at a merchant POS.
2. The equivalent value in bitcoins is debited from the consumer's Coinbase bitcoin wallet. The bitcoin value at the time of purchase is based on the current spot price of bitcoins on Coinbase. There is no transaction fee for converting bitcoins to fiat currency.
3. When the payment transaction is approved, the merchant receives payment in U.S. dollars.

3.4 Interbank Funds Transfer

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Use of blockchains to move funds between financial institutions: Financial institution to financial institution Person to person Person to business Business to business	Faster and more real time Lower cost	Financial institutions Individuals Businesses Networks Technology providers Current funds transfer providers or entities (ACH, Fedwire, SWIFT)	Scalability Reliability Security Perception Regulations	Ripple IBM Hyperledger (Linux Foundation)

Consumers and businesses have been transferring funds between financial institutions for years, both between their own accounts at different institutions and to and from their own accounts and other accounts. The two primary methods of enabling interbank funds transfers within the U.S. are Fedwire and the Automated Clearing House (ACH). Outside of the U.S., the Society for Worldwide Interbank

Financial Telecommunication (SWIFT) provides a network used by over 11,000 financial institutions in more than 200 countries.

Businesses are the largest users of wire transfers. A total of 287.5 million wire transfers were completed in 2012 with a value of $1,116.3 trillion.[17] The number of ACH transfers in 2014 totaled almost 23 billion, with a value of more than $40 trillion.[18] Appproximately 3 billion of the ACH transfers were associated with bill payments initiated through online banking websites (or directly through billers) and settled over ACH.[19]

Most interbank transfers are processed through wholesale payment systems, which handle large-value transactions between banks, both on their own behalf and for the benefit of others. The Clearing House Interbank Payments System (CHIPS) and Fedwire are used to move these funds within the U.S. SWIFT enables cross-border transactions and moves funds between countries. During 2015, SWIFT processed over 6.1 billion messages.[17]

One of the challenges of interbank funds transfers is the inability to clear and settle transactions quickly. While some of the underlying services enable so-called "immediate" transfers of funds between financial institutions, the reality is that the process can sometimes take hours or even days. How to make payments faster (and more secure) is a current topic in the industry, both in the U.S. and worldwide. The stated objective of the Federal Reserve's Faster Payments Task Force[20] is to "identify and evaluate approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States." Much of the initial focus of that group is on interbank funds transfers. Similarly, the goal of the same-day ACH initiative,[21] currently underway, is to "provide a ubiquitous same-day clearing and settlement capability for virtually all ACH payments."

Another challenge is the use of centralized entities to enable interbank transfers. A centralized entity represents a potential single point of vulnerability as well as higher infrastructure costs and higher prices.

3.4.1 Implementation Challenges and Considerations

Blockchain technology could provide a ledger that tracks interbank transfers and could enable these transactions to take place without the current number of intermediaries. These services could include:

- Bank to bank transfers
- Business to business transfers
- Consumer and business wire transfers
- Bill payments made through a bank's online banking service or directly on a biller's website

Many of the current transfer systems have been in use since the 1970s. Using blockchain technology could potentially lower the costs of maintaining the ledger or accounting for the transactions and further secure tracking and auditing (since entries cannot be deleted). It could also eliminate the need for centralized entities or "middlemen."

[17] Federal Reserve Payments Study press release, July 24, 2014.
[18] NACHA press release, April 15, 2014.
[19] Federal Reserve Payments Study press release, op. cit.
[20] https://fedpaymentsimprovement.org/faster-payments/
[21] https://resourcecenter.nacha.org/

Both technology providers and owners of the companies who enable a large portion of interbank transfers have already invested in blockchain technology or announced plans to provide solutions to enable faster payments between financial institutions.

For example, IBM announced that it will be testing its own blockchain-based transaction system.[22] The technology provider Ripple enables banks to transfer funds between each other without the need for an intermediary (Figure 1).[23] In addition, several new entrants who have implemented the underlying blockchain technology plan to submit proposals to the Federal Reserve in response to the faster payments initiative. Microsoft is working with a number of large banks and a company called R3 to move assets around using bitcoin-inspired software within their cloud computing platform, Azure. Although the initial focus was on securities clearing, the effort appears to be expanding.

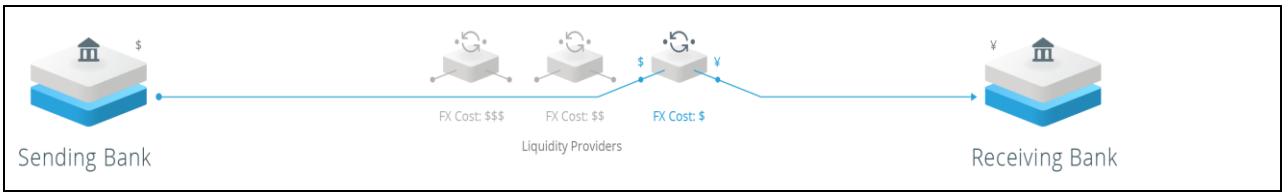

Figure 3. Ripple's Distributed Technology

However, replacing current processes and systems with blockchain solutions can add new challenges.

First, many stakeholders will need to embrace the use of blockchain to conduct interbank funds transfers, and blockchain still has a somewhat checkered reputation, due to its close ties to bitcoins and industry inexperience with the technology. Relevant stakeholders include financial institutions, large and small businesses, consumers, the federal government (due to regulatory requirements for interbank funds transfers) and technology companies with offerings that currently facilitate interbank funds transfers. In addition, current regulations (e.g., Know Your Customer, Anti-Money Laundering) will probably need to be updated to support the widespread use of blockchain for interbank funds transfers.

Another complication is that while many financial institutions are involved in trials and proof-of-concept exercises, there is no established business case to justify the mass use of blockchain for interbank funds transfers. An additional concern is that consumers and businesses want to ensure that transactions involving their finances are confidential and secure. Widespread adoption of any new technology, including blockchain, requires education and trusted advisors to assure consumers and businesses that their transactions are secure and protected.

Finally, concerns about scalability and reliability may increase as the use of blockchain expands beyond current niche solutions.

3.4.2 Real World Examples

While as yet there are no "live" examples of using blockchain for interbank fund transfers, proof-of-concept examples are expected soon. Several solutions at the Federal Reserve Faster Payments Capability Showcase use blockchain technology, and it is possible that a blockchain solution is one (or more) of the 22 solutions that have been submitted to the Federal Reserve Faster Payments task force.

[22] Robert McMillan, "IBM Bets on Bitcoin Ledger," *The Wall Street Journal*, Feb. 16, 2016, http://www.wsj.com/articles/ibm-bets-on-bitcoin-ledger-1455598864.
[23] https://ripple.com/.

Several recent announcements and activities also support the idea that blockchain is a potentially viable technology for such transfers:

- On Feb. 25, 2016, Royal Bank of Canada announced that it was working on a new proof of concept for distributed ledger-based remittances using technology offered by industry startup Ripple.[24]
- J.P. Morgan Chase & Co. announced in February 2016 that it is testing technology that underpins bitcoin-to-U.S.-dollar transfers between London and Tokyo.[25]
- On Feb. 9, 2016, the Linux Foundation announced that several new members from across the industry are participants in the Foundation's Hyperledger Project (an open source project to advance blockchain technology).[26]

3.5 Asset Registry

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Use of a blockchain asset registry to be the primary and immutable source of ownership information for property such as land, high value durable goods, and equities. The blockchain can facilitate real-time transfer of and payment for assets.	Real-time auditing Reduced costs Speed Security Transparency Instant ownership/ transfer Immutability	Exchanges Government agencies: land title offices; taxation authorities Consumers Businesses	Constituent buy-in Establishment of a baseline Consistent and reliable access (e.g., power) ROI perception	Republic of Georgia Nasdaq Ghana SETL, Metro Bank, Deloitte

Another promising application for blockchain technology is its use for implementing an asset registry. A blockchain asset registry can act as the primary and immutable source of ownership information for property such as land, high value durable goods, and equities. The blockchain can also facilitate real-time transfer of ownership and payment for assets.

Asset registries tend to be very labor- and paper-intensive. Introducing blockchain solutions to this space will no doubt shake up the status quo. The efficiencies in process and speed as well as expense bring many opportunities for companies offering solutions in the market.

[24] http://www.coindesk.com/royal-bank-canada-reveals-blockchain-remittance-trial-ripple/

[25] "JPMorgan Quietly Tests 'Blockchain' With 2,200 Clients," Wall Street Journal, Feb. 22, 2016, https://www.wsj.com/articles/one-place-j-p-morgan-is-boosting-spending-fintech-1456172040

[26] "Founding members of the initiative represent a diverse group of stakeholders, including: ABN AMRO, Accenture, ANZ Bank, Blockchain, BNY Mellon, Calastone, Cisco, CLS, CME Group, ConsenSys, Credits, The Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, Digital Asset Holdings, Fujitsu Limited, Guardtime, Hitachi, IBM, Intel, IntellectEU, J.P. Morgan, NEC, NTT DATA, R3, Red Hat, State Street, SWIFT, Symbiont, VMware and Wells Fargo." Linux Foundation, "Linux Foundation's Hyperledger Project Announces 30 Founding Members and Code Proposals To Advance Blockchain Technology," Feb. 9, 2016. http://www.linuxfoundation.org/news-media/announcements/2016/02/linux-foundation-s-hyperledger-project-announces-30-founding.

3.5.1 Implementation Considerations and Challenges

Blockchain asset registry implementation options are somewhat limitless. Registering land ownership, establishing equities ownership and executing equity trades are just a few of the examples outlined in this section, but the domain of registrable assets is nearly as big as the pool of all non-fungible goods. As more registry implementations go live, natural markets will surface based on the relative value and usefulness of using the blockchain.

As the insurance industry looks to register policies through blockchain smart contracts, it also seeks to leverage blockchain solutions to track the actual insured assets. For example, fine art and diamond dealers are working to establish ownership ledgers and track owner history with blockchain implementations.[27]

Blockchain hashing may be one of the greatest assets in moving forward with tracking and true identification and certification of high value assets. In a space where fraud is camouflaged and where proving authenticity can be difficult, the hash may bring some comfort. Whether a precious gem or a priceless painting, the elements that make it truly unique may just be the data elements used in the mathematical hash that allow the original to distinguished from a counterfeit.

The true mark of the blockchain in the asset registry space will be the solutions and implementations not yet envisioned: the opportunities to leverage the blockchain for new and exciting uses well beyond solving today's known problems.

Challenges for blockchain asset registries will range from technical and logistical to very real and potentially immovable personal and bureaucratic beliefs. For example, if the goal is land titling in a developing country, there will no doubt be some struggle with establishing a reliable infrastructure, like electricity and network connectivity. Additionally, these land efforts may run into political roadblocks. In some cases, the absence of reliable land titling has left the door open for significant corruption and illegal transfer of land assets. Bringing in a definitive source to track land ownership will eliminate the foundation on which that corruption was based.

Asset registration on the blockchain will also need to address the challenge that comes with converting from certificate- and paper-based ledger systems. Not unlike the journey of paper medical records to electronic medical records, blockchain asset registry efforts will struggle with the best way to establish a baseline.

3.5.2 Real World Examples

Blockchain asset registries are being implemented in a variety of locations and for a variety of purposes.

3.5.2.1 REPUBLIC OF GEORGIA: LAND TITLING

The Republic of Georgia, in partnership with BitFury, is building a land titling infrastructure based on blockchain technology. "By building a blockchain-based property registry and taking full advantage of the security provided by the blockchain technology, the Republic of Georgia can show the world that we

[27] http://www.kpmgtechgrowth.co.uk/blockchain-the-power-of-transparency/

are a modern, transparent and corruption-free country that can lead the world in changing the way land titling is done and pave the way to additional prosperity for all."[28]

3.5.2.2 NASDAQ PRIVATE MARKET: OWNERSHIP SHARES

Nasdaq Private Market is piloting Nasdaq Linq, a product that enables private companies to execute pre-IPO trading on a blockchain. Work that is typically manual, time consuming, and costly (and typically requires the participation of lawyers) can be automated and performed quickly without relying on a third party. Entrepreneurs and private investors are able to execute their transactions without the complications of traditional manual or spreadsheet-driven processes that are prone to error. Linq shows ownership shares on a timeline graphic called the Equity Timeline View, which identifies who owns shares as a flowchart. [29]

3.5.2.3 GHANA: LAND TITLING

Estimates show that who owns 78% of the land in Ghana is presently unrecorded. The Bitland (Land Title Protection Ghana)[30] effort partnered with OpenLedger to create blockchain solutions for a variety of situations (e.g., smart contracts, voting), including land titling. It is anticipated that formal titling and ownership assignment will free up capital for mortgages, development, and infrastructure.

3.5.2.4 SETL: RETAIL PAYMENT SYSTEM

SETL, Metro Bank and Deloitte implemented a London-based demonstration of a contactless-smart-card-enabled blockchain allowing digitized payments. Customers taking part created their identity records on the Deloitte blockchain and had their key details certified by Deloitte; these certified details were then asserted to the SETL blockchain to set up user credentials. Metro Bank hosted the customer account. Customers were issued contactless smart cards which were used to make purchases from merchants equipped with contactless terminals. Consumers and merchant balances were updated in real-time with all balances held at Metro Bank.[31]

3.6 Anti-Counterfeiting for Asset Tracking

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Use of blockchain technology to verify origins, history, and authenticity of digital and physical goods	Non-repudiation Low participation threshold for consumers Less lost merchant revenue	Consumers Merchants Manufacturers Distributers Technology providers	Adoption to close the supply chain Platform provider Form factor of unique identifier	Blockverify Everledger

[28] Laura Shin, "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury," *Forbes*, Apr. 21, 2016, http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#7c08862b6550.

[29] Pete Rizzo, "Hands On With Linq, Nasdaq's Private Markets Blockchain Project," Coindesk, Nov. 21, 2015, http://www.coindesk.com/hands-on-with-linq-nasdaqs-private-markets-blockchain-project/.

[30] Bitland Land Title Protection Ghana, http://www.bitland.world/.

[31] "SETL, Deloitte and Metro Bank Put Sterling onto the Blockchain for Consumer Payments," SETL press release, Nov. 15, 2016, https://setl.io/.

Counterfeiting in trade appears to be a real problem; roughly 7–8% of global trade is composed of counterfeit or pirated goods, from consumer (digital) goods to technology products and pharmaceuticals.[32] Counterfeiting accounts for more than $500 billion of lost sales globally. Consumers deserve to be assured of the authenticity of the products they are buying, for which reason these products often include an identifier that authenticates them. However, to be effective, the identifier must be hard to copy and easy to verify.

Current anticounterfeiting solutions fall into one of two categories: either authenticity can be verified without any special equipment (e.g., a unique label or a hologram), or specialized tools or skills are needed to verify product authenticity (e.g., watermarks or temperature-sensitive inks). However, modern manufacturing techniques are making it easier to outwit both approaches. Blockchain technology represents an alternative solution to the counterfeiting problem.

3.6.1 Implementation Considerations and Challenges

Using block chain technology to combat counterfeiting might work as follows:

1. The manufacturer (sender) completes the product.
2. The manufacturer sends the product to the retailer (receiver).
3. Simultaneously with the physical transaction and product shipment, the manufacturer performs a blockchain transaction.

Such a process prevents fraudulent transactions by verifying product ownership. The full history of the product, its components, and any transfer of ownership is recorded in the distributed ledger (blockchain) and can be verified by anyone with access to the ledger. Any diversion from the product's intended path can be observed clearly, making it easier to track and identify stolen goods. The entire process is transparent, and there is no need to base product authenticity on trust only.

To translate the physical into the virtual, the product could, for example, be labeled with a unique number. As the product ships from one member of the supply chain to another, the number is signed with the sending member's private key. Consequently, it is possible to trace the entire path of the product.

For example, assume the number is displayed as a QR code. On receiving the product, a retailer can verify the full history of the product. Scanning the QR code provides the retailer with information to verify the signature of the product's sender, making it easier to recognize counterfeit products. The verification process can take a variety of forms, but technically only an online portal or mobile phone would be required to enter or scan the unique number and verify the path (and thereby the authenticity) of the product. Such a verification system can be open to everyone, restricted, or a combination of both (hybrid). In order to prevent modifications of the number by physical means, an SE could be used to store a secret specific to the device and allow it to be securely identified.

The proposed solution is not free of challenges. One issue is whether to make the ledger public, private, or a combination. A hybrid ledger is preferable, with the public portion accessible to consumers and the private portion accessible to manufacturers and suppliers.

The challenge for businesses is implementation. A manufacturer, bulk buyer, or any other member of the supply chain would have to participate in the process and be willing to make the effort required to

[32] STOPfakes.gov, "Learn about IP: How serious a problem is counterfeiting and piracy?," http://www.stopfakes.gov/learn-about-ip/ip/how-serious-problem-counterfeiting-and-piracy.

implement such a solution. In addition, whether consumers accepted a blockchain-based solution could prove to be critical to success.

3.6.2 Real World Examples

Blockchain implementation for anticounterfeiting applications is being developed by several startups. Applications support the diamond trade (to verify the origins of a stone), pharmaceuticals, electronics, and other luxury items.

3.7 Internet of Things

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations and Challenges	Real-World Examples
Use of blockchain technology to record transactions based on autonomous decisions made by IoT nodes	Autonomous action by IoT sensors	Product makers IoT network developers	Development of the blockchain infrastructure	IBM ADEPT Samsung washing machine Filament

Blockchain technology can be used by a node on the Internet of Things (IoT) to record services requested autonomously. Because both the IoT and blockchain technology are still young, numerous potential applications have yet to be identified. For example, a blockchain could be used to track the history of data exchanges between individual devices, storing specific requests in a ledger.

3.7.1 Implementation Considerations and Challenges

Blockchain technology can be used to implement automatic initiation of low cost transactions (which are typically also low risk transactions). Such transactions can be initiated automatically by a sensor, without a requirement for human intervention. For example, a sensor located in a particular field on a farm could tell the farm's irrigation system that the area is dry, and initiate irrigation in that area alone rather than on the entire farm, without involving the farmer. Blockchain technology can be used to verify that the request indeed came from an appropriate source.

Blockchain technology can also be used to enable a device to accept payment without involving a person in the transaction. For example, Company A could place a sensor at an inconvenient location (such as the top of a mountain). When the rainfall data Company A collects at that location is needed by Company B to determine how much water to release from a dam in the valley, the sensor could be paid for the data by Company B's sensor. Using blockchain technology, payment would be recorded in the ledger and then verified.

One of the major challenges is scalability. When blockchains become too large, they can be unwieldy and delay system-critical processes. Currently there is no agreed-upon standard that addresses the scalability problem. Efforts such as sidechains and treechains have both benefits and drawbacks.

Another challenge is the requirement for computing power. Blockchain security requires massive computing power when based on proof of work. However, there is active research to find more cost-effective alternatives to keep the system secure (e.g., Ethereum Casper).

3.7.2 Real World Examples

IBM has unveiled a proof of concept for ADEPT, a system that relies on blockchains to build a distributed network of devices. The system relies on a mix of blockchain techniques to secure transactions.[33] Samsung has designed a washing machine that uses the IBM framework to order needed supplies from a vendor automatically.

Filament is a company that uses blockchain and other technologies to create a network of connected devices that can transfer data autonomously.

[33] Stan Higgins, "IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things," CoinDesk, Jan. 17, 2016, http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/.

4 Challenges for Blockchain Implementations

Using blockchain technology for any of the implementations described in this white paper is not without challenges. Important considerations include:

- Permissioned or permissionless blockchain
- Scalability
- Standards
- Security considerations
- Reputation and consumer perception
- Legal and regulatory considerations

4.1 Permissioned or Permissionless Blockchain

One consideration is whether an implementation should rely on a permissioned (private) or permissionless (public) blockchain. Early blockchain implementations were permissionless networks. Anyone in the world could join in, and transactions were guaranteed by proof-of-work data combined with consensus. Being trustless is one advantage of a permissionless network, but there are disadvantages. For example, the computational intensity of mining compromises the network's efficiency and scalability, and governance is achieved only by miner consensus, making it difficult to agree on network improvements.

As a result, many financial institutions are experimenting with permissioned networks, of which startups like R3, Eris, Hyperledger, and Ripple are examples. These implementations may be more efficient, without the need for mining. They benefit from transaction immutability and not having a single point of vulnerability. However, a permissioned blockchain requires trust between the network nodes.

4.2 Scalability

Another consideration is scalability. Bitcoin, for example, is facing some limitations. Currently, Bitcoin can manage approximately 10 transactions per second, compared with Visa's volume of 3,200 transactions per second.[34]

Several paths are being explored to augment this number. One solution for Bitcoin could be to increase the number transactions per block. This question is currently disputed within the Bitcoin community.[35] If the block becomes too large, the system may need to be consolidated and restricted to nodes that are capable of handling larger blocks.

Scalability depends on how the blockchain is being used. Scalability is a more serious issue in permissionless networks. In a permissioned network, there might be trust between the network nodes, so the underlying assumption is that no actor within the network is malicious. The network is easier to enlarge: it can simply add nodes as they become trusted. In a permissionless network, where nodes can join or leave at will, the network must be robust enough to withstand a 51% attack. To prevent such an attack, the hash rate must speed up quickly; the cost is that software must be added to less specialized, and therefore slower, equipment.

[34] 100.8 billion total transactions over the four quarters ending on March 31, 2015. VISA, "Visa Inc. at a Glance," https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.

[35] Mike Hearn, "The resolution of the Bitcoin experiment," Medium, https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.i6ttzevna.

4.3 Standards

Currently, few standards are applicable to blockchains. Each altcoin in the marketplace is attached to a different blockchain. The smaller an altcoin, the more susceptible it is to a 51% attack. To create a new blockchain from scratch would require significant investment by an institution to set up a network with enough hashing power to prevent a takeover. Alternatively, the network could consist of trusted nodes. However, there must be agreement between the users as to the type of blockchain to use. Several startups can create blockchains for specific use cases, but for the blockchain to be viable, users must accept it.

One initiative has been announced, a consortium including Cisco Systems, Bosch Ltd and several other companies, to develop a shared blockchain protocol for the IoT.[36] In addition, some technology providers are moving forward with technologies that are similar to blockchain but with a different focus, such as R3 Corda™,[37] which uses a distributed ledger platform rather than blockchain technology.

4.4 Reputation and Consumer Perception

In the eyes of the public, blockchains mean Bitcoin, which has become notorious through Silk Road and other websites. Furthermore, blockchains are highly technical, which may make the idea difficult for the average consumer to understand. All of these factors may discourage consumers from wanting to use blockchain applications, unless they are offered by a trusted entity such as a bank.

Many of the use cases described in this white paper require that the blockchain be trusted by the participants. The issue of trust raises additional considerations. If the blockchain is permissioned, who grants permission? If it is permissionless, what guarantees that no 51% attack can be carried out? For example, a land title system relying on a permissioned blockchain could be run by a government. However, a malicious or corrupt participant could change the titles. Conversely, if the blockchain is permissionless, the reward for miners would need to outweigh the potential gain from acting maliciously.

4.5 Security Considerations

The security of a blockchain relies upon a strong consensus mechanism, which must ensure that the system behaves correctly as soon as a majority of participants behave honestly. This consensus must also allow good system performance, which can sometimes contradict the security requirement; consensus algorithms have to be finely defined to ensure both security and efficiency. This is still an active research area.

An important characteristic of proof-of-work based consensus, like the one used by Bitcoin, is the hash rate achievable by the network. If the hash rate is too low, it is easier for some malicious party to surpass the network hash rate and achieve a 51% attack; malicious actors could then rewrite transactions or prevent new transactions from occurring. This risk is principally present early in the deployment of a proof-of-work blockchain, when there are only a few nodes on the network. The resources required to attack the blockchain are much lower at that time than what is required to attack a more developed network. These risks can be avoided by implementing a permissioned network, where only trusted entities are allowed to update the blockchain.

---

[36] http://www.reuters.com/article/us-blockchain-iot-idUSKBN15B2D7.

[37] Richard Gendal Brown, "Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services," R3, Apr. 5, 2016, http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services.

Bitcoin's hash rate[38] is 3,023,758 TH/s (1 billion hashes per second) as of Feb. 22, 2017.[39] This number makes a 51% attack infeasible on Bitcoin, in theory. In practice, Bitcoin miners are organized in "mining pools." As the hash rate increases, solving the proof-of-work first becomes difficult and requires investments in specialized hardware. That is why miners have regrouped in pools: they work together on proofs and share the earnings based on how much work they have performed. A "pool manager" coordinates the work, so that efforts are made on the same block. The advantage of pools is that they allow smaller miners to participate. The inconvenience is that pools might become too powerful; in January 2017, more than 51% of the hash rate was produced by four pools. This mining centralization can be viewed as a risk, as colluding pools could easily control the blockchain.[40]

Recent research has also shown that, in some conditions, miners can profit from dishonest behavior even if they control only a small part of the mining power. However, this kind of behavior, as well as colluding pools, has not been observed in practice. These risks potentially exist for all blockchains, but attackers are discouraged by the fact that expected gains are actually higher with an honest behavior. Incentives play a central role in blockchains: they should be so that the best strategy for all miners is the honest one. Transaction fees provide these incentives. One would also note that a 51% attack would be highly visible in the network, and that attackers care about the exchange rate of Bitcoin, which would drop if trust in the blockchain decreases.

On the user's side, a big security risk is the storage and management of private keys. If a private key is compromised, all transactions will seem to come from the correct person. To address this risk, private keys should be generated and stored in secure hardware, like a smart card or secure element on a mobile device, preventing the key from being compromised while allowing for the signing of transactions. A backup procedure must also be put in place.

4.6 Legal and Regulatory Considerations

The U.S. Senate started hearings on Bitcoin in 2013, and in 2014 the IRS clarified tax treatment for Bitcoin. The State of New York published a "BitLicense" paper in April, 2015, the first in the world directed at virtual currencies.[41] This was considered important since New York is the country's financial center. How New York approaches Bitcoin will impact investor attitudes and other states will look to New York for guidance when deciding how the approach for their own state. One of the aspects addressed in the New York paper was general capital requirement guidelines, intended to prevent exchanges from running unreported deficits, as Mt. Gox did.[42] In late 2016, New York also announced the nation's first cyber security regulation that impacts virtual currency companies.[43]

After a flurry of publicity and rumors circa 2013-2015, it has been somewhat quiet since. The UK seemed to step ahead of the U.S. with its BitLicense in 2016, offering the ability for UK FinTechs to operate throughout the European Union (EU),[44] but of course this advantage likely evaporated with the passage of Brexit.

---

[38] The hash rate for different blockchains depends on which hashing algorithm is used (e.g., KECCAK-256, SHA-256, scrypt), which means that the hash rate for one blockchain cannot necessarily be compared with the hash rate for another accurately.

[39] https://blockchain.info/charts/hash-rate.

[40] https://blockchain.info/en/pools

[41] https://bitcoinmagazine.com/articles/the-united-states-is-falling-behind-in-bitcoin-regulation-1461604211/.

[42] https://www.cryptocoinsnews.com/final-new-york-bitcoin-regulation-released-bitlicense/.

[43] https://cointelegraph.com/news/us-first-cyber-security-regulation-to-pressure-bitcoin-companies.

[44] https://bitcoinmagazine.com/articles/the-united-states-is-falling-behind-in-bitcoin-regulation-1461604211/.

Banks often refuse to serve virtual currency companies due to uncertainty. Firms that control customer funds must obtain money transmitter licenses in each of at least 48 states, a cumbersome, expensive process that is a barrier to startups.[45]

Some of the difficulties involved in regulating virtual currencies include[46,47]:

- Lack of understanding of the technology
- Determining the nature of virtual currency. Is it a commodity or a currency, or both?
- The need to update bankruptcy and other laws to reflect a new way of conducting transactions
- Vast variety of regulatory treatment across countries, ranging from taxing it to outright bans

The resulting patchwork of state regulations include:[48]

- Refusal to grant a money transmitter license to virtual currency companies (Wisconsin)
- Requirement for a money transmitter license, which is considered unfavorable to virtual currency (North Carolina, California, Pennsylvania, Florida, New Mexico, Georgia, Connecticut, Washington, New York, New Hampshire)
- Making Bitcoin illegal (Hawaii)

All other states are considered to be grey areas, or have no money transmitter license laws. Thus, some in the industry are saying that the lack of certainty and cumbersome patchwork of expensive U.S. regulation are driving blockchain companies outside of the U.S.[49]

[45] https://blog.coinfund.io/how-will-the-united-states-regulate-cryptocurrencies-and-blockchain-technology-5f69ccc3da7b#.qv6lo61nb
[46] http://www.huffingtonpost.com/john-rampton/why-bitcoin-is-not-regula_b_9458864.html
[47] https://www.wired.com/2016/03/must-understand-bitcoin-regulate/
[48] http://news.dinbits.com/2017/01/state-of-regulation-2017-bitcoin-and.html
[49] http://www.forbes.com/sites/perianneboring/2016/06/28/the-blockchain-brain-drain-how-the-states-are-driving-blockchain-companies-abroad/#113a638a884e

5 Conclusions

Blockchain technology is widely viewed as revolutionary due to the ingenious way it solves for a transparent, distributed consensus network that is resistant to manipulation or takeover by a central authority. As a result, FinTech startups, financial institutions, and technology companies have invested in blockchain at an unprecedented rate—more than $1 billion since 2009—and this investment is still accelerating dramatically. Blockchain has been dubbed by industry analysts the fastest development software market in history. New blockchain applications are still emerging, and use beyond digital currencies is still being defined. Blockchain implementation for financial services applications is expected to be a significant area of growth. Financial institutions are expected to spend more than $1 billion in 2017 on blockchain applications[50] and increasing numbers of large banks around the world are experimenting with blockchains and bitcoins. Financial services expected to use blockchain are: real-time settlement; money transfer; and smart contracts.

Blockchain's crucial innovation is a decentralized ledger, secured with cryptography, that ensures integrity, immutability, and no single point of vulnerability in the network. However, one remaining area of vulnerability is the private keys associated with ownership. If those private keys are lost or stolen, any associated coins or assets are lost forever. Many people have inadvertently erased their private bitcoin keys, and the associated bitcoins have essentially disappeared. In other cases, thieves have hacked into centralized exchanges, stolen private keys, and irretrievably transferred the assets.

Secure element and smart card technology can play a critical role in securing blockchain transactions in certain use cases, including cryptocurrencies and vaults, funds transfer, asset tracking, and the Internet of Things. Since blockchain applications may include the ability to execute contracts and make transactions, they must be secure: secret keys are used and need to be secured. Secure element technology, available in different form factors, can be used to generate, secure and manage these secret keys. Real-world examples include:

- Plutus uses NFC to "tap and pay" with bitcoin at any POS that accepts fiat currency.
- Several bitcoin debit cards perform transactions using EMV contact or contactless technology, including BitPlastic, Coinkite, and Cryptopay.
- Several implementations use hardware-based vaults to secure private keys. These include Ledger, which stores the key in an SE residing on a USB device.

As blockchain technology continues to evolve, the Secure Technology Alliance envisions a future in which smart card technology, in partnership with blockchain technology, can enable straight-through transactions with dramatic improvements in safety, security, and integrity.

[50] Magister Advisors, "Blockchain & Bitcoin in 2016 - A Survey Of Global Leaders," December 2015, http://www.slideshare.net/jeremysmillar/magister-advisors-blockchain-bitcoin-in-2016-a-survey-of-global-leaders.

6 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to provide a primer on blockchain technology, discuss use cases that are currently commercially available or being piloted, and discuss the role secure element/smart card technology plays in the different use cases.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: Capgemini; CH2M; Consult Hyperion; CPI Card Group; Discover Financial Services; First Data; FIS; Fiserv; Gemalto; GlobalPlatform; Infineon Technologies; Ingenico Group; Kona I; NextGen ID Inc.; NXP Semiconductors; Oberthur Technologies; PayGility Advisors; Quadagno & Associates; Rambus; SHAZAM; Underwriters Laboratories (UL); Verifone; Visa, Inc.

The Secure Technology Alliance thanks Council members who participated in the project team to write the document, including:

- **Andreas Aabye**, Visa
- **Philip Andreae**, Oberthur Technologies
- **Suresh Bachu**, Discover Financial Services
- **Deborah Baxley**, PayGility Advisors
- **Maarten Bron**, UL
- **Jose Correa**, NXP Semiconductors
- **Terry Dooley**, SHAZAM
- **Emmanuelle Dottax**, Oberthur Technologies
- **Allen Friedman**, Ingenico
- **Imran Hajimusa**, Verifone
- **Simon Laker**, Consult Hyperion
- **Cathy Medich**, Secure Technology Alliance
- **Docia Myer**, CPI Card Group
- **Manish Nathwani**, SHAZAM
- **Todd Nuzum**, NXP Semiconductors
- **Michael Poitner**, NXP Semiconductors
- **Peter Quadagno**, Quadagno & Associates
- **Lokesh Rachuri**, Capgemini
- **Brian Stein**, CH2M
- **Sridher Swaminathan**, First Data
- **Minaoar Hossain Tanzil**, Kona I

The Secure Technology Alliance also thanks Council members who participated in the review of the white paper including:

- **Hank Chavers**, GlobalPlatform
- **Todd Freyman**, Rambus
- **Jack Jania**, Gemalto
- **Umesh Kulkarni**, FIS
- **Tom Lockwood**, NextGen ID Inc.
- **Oliver Manahan**, Infineon Technologies
- **Sherif Samy**, UL
- **Jamie Topolski**, Fiserv

Trademark Notice

About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments

industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.