A Blockchain Buyer's Playbook Part 1

Compliments of

INFOSIGHT®
www.InfoSightInc.com
20 YEARS

SEPTEMBER 21, 2019

Caplock Security LLC
Tuan Phan, CISSP, CBSP, PMP, Security+, SSBB

CAPLOCK SECURITY

Introduction

Blockchain may offer many benefits to an organization; here's what you need to know before you buy in.

When Bitcoin topped $10,000 in 2017, the cryptocurrency made headlines, catching the worldwide attention beyond technology enthusiasts and crypto-miners and cryptocurrency traders. At the same time, blockchain technology, the technology behind the Bitcoin was touted to the mainstream audience as possessing the potential to impact business in various ways, from recordkeeping processes to transaction tracking and many back-office activities such as asset management, procurement, inventory, financial reporting and tax preparation, just to name a few. However, there is more to know about blockchain than Bitcoin.

Let's start the discussion with some basic inquiries.

What is Blockchain?

According to a recent survey conducted by ZDNet's Tech Pro Research (June 18, zdnet.com), 64% of the professionals responding, expect blockchain technology to impact their industry in a positive way, but 70% have not utilized any form of blockchain technology. In addition, most responders may cite Bitcoin as an example of blockchain, there are different "flavors" of blockchain technology as well as possible use cases and implications for the early adopters from variety of perspectives such as scalability, regulatory, security and privacy.

In the book, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World" (Portfolio, 2016), authors Don and Alex Tapscott describe the blockchain technology as "an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." Wikipedia defines blockchain technology as "a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network."

A security engineer or developer can think of blockchain technology as a distributed database where the records are continuously updated and reconciled by all participants using a peer-to-peer protocol within the network. The reconciliation process maintains the integrity of the database disallowing records that have not been accepted as valid by the blockchain network. Several platforms of blockchain technology are available in the marketplace including Ethereum, Ripple, R3 Corda, and Hyperledger derivatives such as Fabric, Sawtooth, Iroha, Burrow, and Indy.

Blockchain Technology at Work

Business use cases of blockchain technology start with Bitcoin anonymous inventor Satoshi Nakamoto' 2008 publication, "Bitcoin: A Peer-to-Peer Electronic Cash System," a system to facilitate online payments from one party to another without the need for an intermediary such as a financial institution. It is difficult to disagree that blockchain technology is appropriate for managing cryptocurrencies, especially given there were more than 2,000 cryptocurrencies in existence as of August 2019. Cryptocurrencies thrive in untrusted environments like the internet and in the absence of central authorities, such as the country of the fiat currency or network operator.

However, for blockchain technology to become more widely accepted, its uses must extend beyond cryptocurrencies. Accordingly, drawing from the cryptocurrency space, three possible generic use cases for blockchain applications emerge. The author conducted an analysis of Ethereum public blockchain in early 2019 to further understand the different use cases and found that the applications are related to games, exchanges, and gambling accounted for over 75% of the applications on Ethereum.

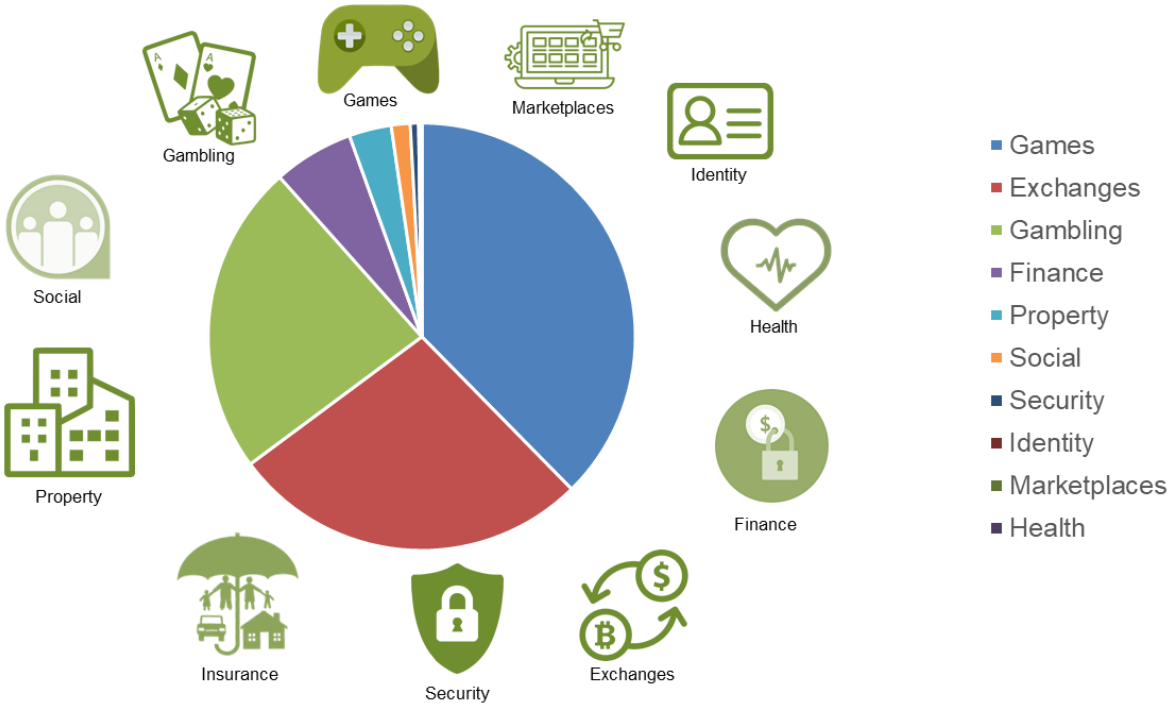


Figure 1 – Use Cases on Ethereum Blockchain

Proof of Existence (and Identity)

The earliest generic use case is proof of existence, which does not consider the time aspect and simply demonstrates the existence of something, regardless of its lifecycle, to offer integrity and assurance of legitimacy. Proof of existence can apply to internet domains, email addresses and corporation/brand names and, conversely, to records such as criminal convictions, debarments, fines and complaints.

Proof of existence can streamline and reduce the friction between multiple systems (e.g., reduction of paperwork burdens, prevention of data errors, reconciliation of transactions) by acting as microservices to handle the finality of transactions among those systems.

Proof of identity may also be viewed as a special case of proof of existence as it leverages identification and authentication to prove identities. Practical applications of proof of identity include:

- Single sign-on services to websites;
- Digital signatures;

- Birth certificates;
- Drivers' licenses;
- Passports;
- Visas;
- Health benefit cards; and
- Other identity-related documentation.

Proof of Chronology

The second generic use case is proof of chronology, which incorporates time and order with the proof of ownership to track transactions over time. Possible applications include the following:

- Regulatory reporting and compliance;
- Accounting and auditing;
- Financial management and procurement;
- Federal personnel workforce data and appropriated funds;
- Federal assistance and foreign aid delivery;
- Clearance/background investigations;
- Professional certifications;
- Marriage certificates;
- Auction/bid processes;
- Clearing and settlement;
- Escrow services;
- Tracking of payments and deliveries; and
- Other goods and services in which time plays a key role in the fulfillment of the transactions (e.g., food spoilage).

Proof of Ownership

The broadest use case for blockchain technology is proof of ownership. This encompasses all transactions that represent the lifecycle from acquisition to transfer of the ownership, thus provides coverage across proofs of existence/identity and chronology. Possible applications include real estate properties, financial instruments, loans, patents and trademarks. Proof-of-ownership applications should only be utilized for situations where ownership may be acquired (e.g., purchased), transferred (e.g., sold) and disputed (e.g., liened), and accordingly, ownership information must exist or be available in a public forum.

Use Cases for Financial Institutions

While the following may not be a complete list of possible applications for blockchain solutions specific to financial institutions, the list highlights the possibilities for future applications.

Know Your Customer (KYC) / Anti-Money Laundering (AML)

Requiring clients to repeatedly provide identifying information can erode customer satisfaction and cause transaction delays. This apply not only to tradition banking services but also mortgages, investments, and migrating or performing transactions from one bank to another. However, it is a necessary evil to combat AML and meet the strict requirements of KYC.

- CULedger's MyCUID using Sovrin's Digital ID Management
- SecureKey Technologies and partnership of BMO, CIBC, Desjardins, RBC, Scotiabank and TD and IBM

Identity verification on the blockchain works as follows. The providers (SecureKey or CULedger) of attributes get paid for each set they provide and have no liability if they are wrong. The requestor of attributes pays for each set requested and generally will request more than one validator to be comfortable with the claims. For example, a telco or a bank (e.g. Requestors) might request name, address and mobile number from a tier one bank (which requires a real-time bank login), but will also request that the mobile device being used by the user has been validated by the telco, and the SIM in the device matches the mobile number of record at the bank. They will also likely request a credit claim from a reputable agency, showing the credit score of the individual is over 700 and that there are no 90 day + delinquencies on file.

The requestor pays for each claim received and has no ability to go back to the provider if the claims have errors. The network manages the billing and provides most of the funds back to the providers of claims.

Users can add a variety of attributes over time and share them when requested to a valid requestor. The user provides explicit consent each time data is requested (i.e., are you willing to share these attributes with this party for this purpose?) Each action is recorded in the ledger and the user receives a secure notification on all actions.

Clearing and Settlement

The centralization of most clearing and settlement procedures make them great candidates for improvement with blockchain, thereby unlock significant cost savings thru. blockchain adoption.

Consider the current case of SWIFT for use in international payments. At the core, SWIFT is essentially a messaging system among banks. So messages get sent, and those messages trigger the movement of money from bank to bank on several hops, depending on where the receiver is and where the sender is. And that whole process can take several days and can eat up several percentage points of the payment amount. If proposed network uses a currency into a native digital format, instead of sending an electronic message,the network can send the assets themselves electronically. If we can do that, then I can pay a supplier in Vietnam as fast as I can send an email to Vietnam. There are several implementation of blockchain-powered institutional payment and settlement infrastructures from SETL, and Euro-Clear. In addition, Citi and CME Clearing's use of a real-time margin funding payment system that enabling a bank to view the collateral in its ledgers in real time, send cash or securities with one click to a clearing house, and receive an immediate acknowledgment.

Trade Finance

Trade finance refers to financial transactions, both domestic and international, which relate to trade receivables finance and global trade. These trade finance transactions include lending, issuing letters of credit, factoring, export credit and insurance. These transactions make up an enormous portion of global trade – approximately 80 to 90 percent of world trade relies on trade finance. Essentially, almost any time goods or services are bought or sold across any border, there is some form of trade finance involved.

As an example, under the current system of trade finance, ABC Company in the United States seeks to import a shipment of goods from supplier XYZ Company in China. The importer needs to pay for those goods but is hesitant to do so before making sure that the goods will arrive as ordered. The exporter is also hesitant to ship the goods, without being certain that the payment will arrive for the goods they supply. Into this impasse steps the importer’s bank, who issues a letter of credit to the exporter via the exporter’s bank promising to pay the exporter’s bank once documents (such as a bill of lading) has been provided by the exporter proving that the goods have been loaded onto the cargo ship, truck, or train. In this way, both the importer and exporter are protected, and the banks take on the role of holding the money for each party.

Why does one consider blockchain for trade finance? One of the difficulties involved with trade finance is the large volume of paper documents that still make up much of the information flow. Banks are seeking to reduce costs and increase efficiency by replacing the flow of paper for trade finance with digital data flows. Conversely, blockchain tech may have ability to streamline the trade finance process. A blockchain is a data structure that allows the creation of a digital ledger of transactions that can be distributed amongst a digital network by using cryptography. This way, each participant on the network can securely amend that ledger without the need for a central authority.

Possible implementation including the following:

A group of European banks, Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Société Générale and UniCredit, was able to complete a series of cross-border financial trades through a jointly developed blockchain platform. The platform enables banks to facilitate trade transactions between their clients (primarily small and medium-sized businesses (SMEs) trading within Europe) by offering greater transparency, more automation and lower risk.

UBS and IBM – Pilot of two trade transactions, in which Audis were purchased in Germany by a Spanish business conglomerate, and raw materials were imported from Austria to Spain by a global leader in textile development.

Deposit and Lending

Crypto-lending/loans are alternative types of financing. Cryptolending is a very new industry with a conservatively estimated sector size of a $4.7B section (loan originated), and it is fast growing. Basically there are two forms currently available:

1. Individuals, who own the cryptocurrency, lend out the cryptocurrency to the platform operator to earn interest payments. Depending on the lending platform, the type of cryptocurrency, and the amount selected, interest rate between 6% to 14% can be obtained vs. traditional banking interest rate of 1 to 2%.
2. The borrower pledges his cryptocurrency as an asset to secure the repayment of the loan. Typically, you don’t need good personal credit or even a bank account, in some cases. But you might end up with high rates your first time, and it can take several days to get your funds. Currently, close to 100% of today’s loans are fully collateralized. This is due to the fact that uncollateralized lending has not yet been developed, so almost the entire space is collateralized at this stage. How much crypto needs to be pledged to borrow more crypto? The current industry standard is 150% but can be as low as 110% and as high as 200%.

Known use cases include:

- Genesis - The biggest player, by total value of loans originated, Genesis capital offers crypto-based financial services to high net-worth individuals and institutions, with a $75,000 minimum loan amount. It can be assumed that a majority of the activity is conducted by a handful of “crypto whales”.
- Celsius - earns profits by lending coins to hedge funds, exchanges, and institutional traders, and by issuing asset-backed loans at an average of 9% interest.
- Maker - allows users to borrow the stablecoin DAI by collateralizing ETH
- Compound - allows users to pool their assets with other lenders on the platform, in order to create a dynamic interest rate based on the pool’s supply and demand.

- Dharma - is a peer to peer lending platform that allows anonymous borrowers to request loans on their own terms, and any lender can originate that loan.
- dYdx - Like other decentralized lending protocols, dYdX allows users to borrow and lend crypto assets, however, with complete anonymity. Use Cases for Financial Institutions.

Cross-border Payments

Cross-border payments typically involve the transfer of money from one country to another. Typically handles thru. a financial institution, an online service like PayPal, or a storefront-based service like Western Union or MoneyGram.

The traditional cross-border payment model relies on SWIFT to handle only the movement of messages along the payment chain. The correspondent banks do the actual debits and credits across the accounts based on the message and to send the value to the final beneficiary. This process typically requires the participation of five parties at the minimum:

1. The sender
2. The sender's bank
3. The correspondent bank to the sender's bank
4. The beneficiary's bank's correspondent bank
5. The beneficiary's bank
6. The beneficiary

To start, as SWIFT guarantees the transaction between the banks via its messages, thus charges a fee for its role to the banks. Each of the involved banks also charges fees for the processing/handling of the transaction. The remaining fees are related to the amount being sent, the corridor of the transaction, and the exchange rate which is based on the volatility of the origination and destination currencies. The aggregation of fees can ultimately result between 5 to 17% of the transaction.

Examples of implementation include:

The blockchain projects of BoC (Jasper), and MAS (Ubin), were developed on two different platforms: Cora (Accenture) and Quorum (JPMorgan). Thanks to the technical support from the two enormous blockchain platforms developed by Accenture and Quorum, the two central banks were able to demonstrate that Payment vs Payment (PVP) settlement was possible without the use of any intermediaries. Through use of Hashed Time Lock Contracts (HTLC), a type of smart contract that returns funds to sender if conditions are not met within a certain time frame, assets are locked or restricted until conditions are not met in full, at which point they are transferred in their entirety to the desired wallet address.

RippleNet and xRapid provide cross-border payments and immediate liquidity across its 200+ financial institution members, thereby solve the inefficiencies related to speed, transparency, and cost Members include Euro Exim Bank, Bittrex, Bitso, Bitstamp, etc. Ripple recently made a strategic investment in MoneyGram with plan to work together to both expand beyond using traditional foreign exchange markets, which requires pre-funding accounts, and to reduce settlement fees as well as settlement times - to pennies and seconds from dollars and minutes.

World Wire allows for financial institutions to clear and settle cross-border payments in seconds. In this solution, two financial institutions transacting together agree to use a stable coin, central bank digital currency or other digital asset as the bridge asset between any two fiat currencies. The digital asset (e.g., Stellar Lumens) facilitates the trade and supplies important settlement instructions. The institutions use their existing payment systems – connected to World Wire's APIs – to convert the first fiat currency into the digital asset. World Wire then simultaneously converts the digital asset into the second fiat currency, completing the transaction. All transaction details are recorded onto an immutable blockchain for clearing.

Interbank Information Network (IIN) from JP Morgan has over 400 participating banks. The IIN focused on minimizing friction in the global payments process, enabling payments to reach beneficiaries faster and with fewer steps to better address the complex cross border payments industry.

Facebook is building its own cryptocurrency, Libra, and payment systems backed by a consortium of large industry players and investment firms to compete in space with

Visa and the like. Libra is a global, digitally native, reserve-backed cryptocurrency built on the foundation of blockchain technology, allowing people to send, receive, spend, and secure their money, enabling a more inclusive global financial system. Facebook claims that small businesses and 1.7 billion unbanked people will benefit.

Insurance

There are four possible categories of application relating to insurance.

- Fraud detection & risk prevention: By moving insurance claims onto an immutable ledger, blockchain technology can help eliminate common sources of fraud in the insurance industry.
- Property & casualty (P&C) insurance: A shared ledger and insurance policies executed through smart contracts can bring an order of magnitude improvement in efficiency to property and casualty insurance (e.g., captive insurance)
- Health insurance: With blockchain technology, medical records can be cryptographically secured and shared between health providers, increasing interoperability in the health insurance ecosystem.
- Reinsurance: By securing reinsurance contracts on the blockchain through smart contracts, blockchain technology can simplify the flow of information and payments between insurers and reinsurers.

Allianz developed a blockchain prototype for the captive insurance market. In a captive insurance a parent group or groups create a licensed insurance company to provide coverage for itself. The prototype demonstrates that international insurance transactions can be significantly accelerated and simplified. Functionalities include cash payments, real-time access of tracked information can be handled through an immutable chain of records using an intuitive, convenient user interface.

Etherisc built a blockchain-enabled insurance products powered by smart contracts. For example, its cryptocurrency-based flight delay program allowed passengers to purchase flight insurance using either cryptocurrency or fiat money such as USD and Euros, then receive payouts automatically after a qualifying event such as flight delay or cancellation. Other products in development include hurricane insurance, crypto wallet insurance, and crop insurance.

Insurwave is a collaboration of several entities including EY, Guardtime, A.P. Møller-Maersk, Microsoft, and ACORD to provide a blockchain-powered marine hull insurance platform. The platform is now in commercial use and was projected to handle risk for more than 1,000 commercial vessels and 500,000 automated transactions in its first twelve months of operation. The group plans to roll its platform out to other types of business insurance in the future, including cargo, aviation, and logistics.

MedRec is a decentralized content management system for medical records from MIT. Rather than storing medical data directly on-chain, it indexes medical records on the blockchain, allowing records to be accessed by providers who have been granted permission. This is meant to help guarantee patient privacy, while creating an audit trail that makes it easy to find and verify patient information on the blockchain.

B3i is a consortium formed in 2016 by some of the biggest names in the insurance and reinsurance areas to explore the blockchain technology. Members include AIG, Allianz, Aegon, and Swiss Re. B3i launched a prototype of a smart contract management system for Property Cat XOL contracts, which is a type of reinsurance for catastrophe insurance. Each reinsurance contract on the platform is written as a smart contract with executable code on the same shared infrastructure. When an event — such as a hurricane or earthquake — occurs, the smart contract evaluates data sources from the participants and automatically calculates payouts to affected parties.

Popular Use Patterns for Evaluations

When considering use cases, organizations can apply the following use patterns in their evaluations. The absence of one or more of the patterns may indicate a poor fit for blockchain applications.

The most important use pattern for an ideal blockchain is the cost of trust currently performed by the ‘trusted’ intermediaries. In the current transaction models, these are entities that operate, safeguard, oversee and ensure transactions for banks, insurance companies, lawyers, etc. Indirectly, they serve as a quasi-central authority to support the networks. However, their participation adds unnecessary transaction costs and controls on the network, both of which conflict with the blockchain's disintermediation and lack of authority value proposition.

The type of data and the methodology for their use also is central.

Decentralization must be chosen over centralization, as the latter requires implicit trust that contradicts blockchain's trustlessness value proposition. Accordingly, managed data must be sharable or be able to exist on a public forum.

The open access serves as notice for any disputes with the claimed ownership information. For example, in the U.S., real estate properties can be readily retrieved from states' department of tax administration because that information is considered public record. In contrast, health, income tax and financial records do not exist in the public domain. In these instances, privacy takes precedence over transparency due to the limited sharing of information. Furthermore, a certain degree of trust must be placed on the network operator who becomes the custodian and facilitator of the sensitive data.

Also central to blockchain's value proposition is the ability to provide immutability and integrity to transactions in a logistic chain. Consequently, transaction data must be available so that the nodes can compute their version of the digital ledger and confirm the transaction history. By limiting access to the data, the certainty of the ledger is diminished. Although it may be overcome by new methods such as SNARKs, more thorough testing is still needed on a larger scale to demonstrate the viability of these approaches.

Blockchain technology still has critical obstacles to overcome, such as enhancing security without compromising network performance and honoring both transparency and privacy.

The Flavors of Blockchain

Blockchain platforms are generally assigned to two categories, public and private, and platforms share certain common attributes.

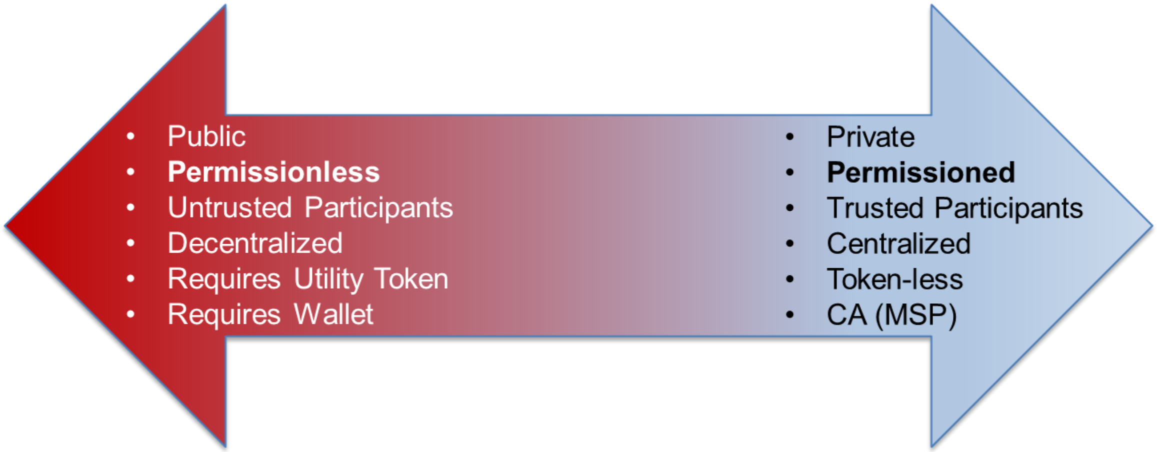


Figure 2 – Public vs. Private Blockchain Networks

Public Blockchain

On one side of the spectrum, a public blockchain is permissionless, where the participants can be anyone if they have the appropriate software to access. Public blockchains operate on a trustless trust model without any central authority. The blockchain network is decentralized or distributed across many nodes or computers, which serve as the communication entities of the blockchain. Since anyone can participate, public blockchain also has the risk of participation from nodes with malicious intent such as stealing cryptocurrencies and compromising integrity and availability of the network.

Public blockchains are less costly to implement as the operators of the nodes bear the cost of the provisioning and maintaining the hardware and software components supporting the blockchain network. The operators, however, are compensated by the network for their ongoing service using native utility token. One or more utility tokens would also be needed for users to consume one or multiple services offered by the public blockchain network. Most notable example of utility token is the use of Ether on the Ethereum network to maintain and execute transactions for decentralized applications (dApps).

Since the public blockchain network is inherently untrusted, the network relies on the user’s private keys of the private/public key pair, typically stored within a virtual or physical blockchain wallet such as JAXX or Ledger Nano S, respectively, to ensure the authenticity of user transactions. Public blockchains disrupt traditional networks by eliminating the intermediaries or middlemen, such as financial institutions in case of Bitcoin, and reduce the overall transaction costs by require no infrastructure costs for creating, maintaining or running dApps.

Private Blockchain

On the opposite spectrum is the private, or permissioned blockchain where participants are known to the network operator and other members. In contrast to public blockchains, private blockchains are semi- to fully-trusted networks, depending on the design, and centralized across a smaller set of nodes/computers. Private blockchains may contain participants across multiple organizations (in case of a federated or consortium blockchains such as R3 Corda and Ripple for financial institutions), or only participants within an organization or network of providers, thereby providing transaction privacy to the members.

Conversely, private blockchains are more costly to implement and maintain as the operating costs are absorbed by its members, but the design is highly scalable and best suited for situations where compliance to data privacy rules and other regulatory requirements is needed. Private blockchain is ideal for governmental information including, but not limited to procurement, credentials such as visas, passports, birth certificates and federal workforce data. Unlike public blockchains, private blockchains do not disrupt the intermediaries but reduce the transaction costs and data redundancies by simplifying data handling and compliance mechanisms of interconnected systems for the participants.

Most private blockchains are token-less and, generally, do not require the use of a blockchain wallet as participants are authenticated through an implementation of public- key infrastructure (PKI). For example, in Hyperledger Fabric, a central entity controls group membership and issues certificates to peers and participants for conducting and validating transactions.

Architecture of a Blockchain Platform

Regardless if the blockchain network is public or private, the blockchain shares four core building elements as follows:

1. Shared Ledger
2. Cryptography
3. Consensus
4. Business Logic

Shared Ledger

1. Shared Ledger deals with how the platform maintains a history of all transactions. Every transaction must be verified before being time-ordered and finalized into a block of valid transactions. The valid block (based on the consensus model to be discussed) is then broadcasted to nodes within the network. The valid block is appended using cryptographic hashes to link to the previous blocks forming a chain of blocks over time (refer to Figure 2), or more commonly known as the shared ledger, serving as immutable records of past transactions. Immutability of transactions enhances the provenance and transparency of information for all participants in the network as they can be certain that information has not been altered.

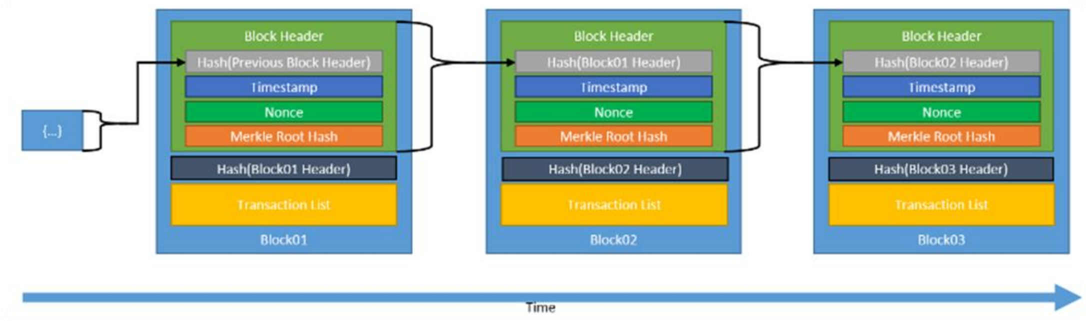


Figure 3 – Generic Chain of Blocks from NISTIR 8202

Each node within the network maintains its own version of the shared ledger. As with distributed networking technology, leads and lags will likely to occur and newly mined blocks may not replicate to all nodes. In such situations, most blockchain platforms will wait until the next block is generated and adopted the longer chain as the official one. The shared ledger's decentralized approach makes the blockchain technology highly resilient and with no single point of failure.

Cryptography

2. Blockchain technology uses familiar and proven cryptography techniques to ensure the integrity of the ledger, the authentication of transactions, and high availability of the network. The blockchain platform relies on nodes to produce transactions and runs a consensus protocol to construct the ledger, which is distributed over a peer-to-peer network. Nodes communicate to neighboring nodes using a gossip protocol ensuring rapid blocks replication across nodes of the blockchain network. Asymmetric cryptography is utilized where private keys are used to digitally sign transactions performed by the users. Participants of the network, in case of public blockchains, are identified by addresses derived from the hash of their public keys. In contrast, private blockchains rely on digital certificates issued by the membership service providers to authenticate participants and nodes. In either case, public/private keys provide the ability for the blockchain to verify that the user transferring value to another user is authorized to sign the value or attest to the ownership.

Consensus Models

3. Consensus is the process by which blocks are accepted and added to the blockchain. This is an important concept as the blockchain does not have a trusted third-party to give the state of the blockchain. The consensus protocol provides the rules from which participants or nodes to derive a common agreement over time. The most common consensus models are:

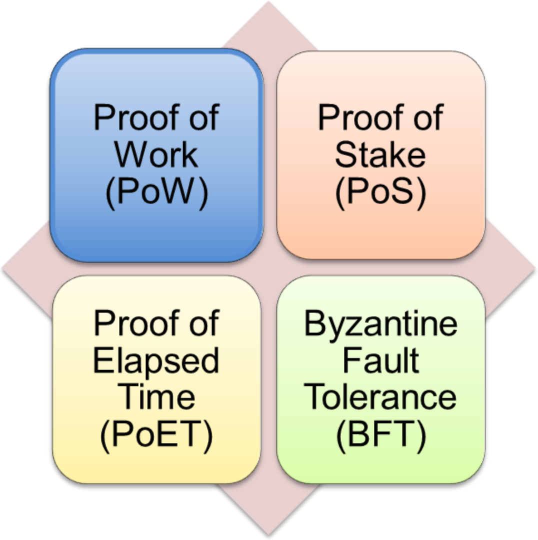


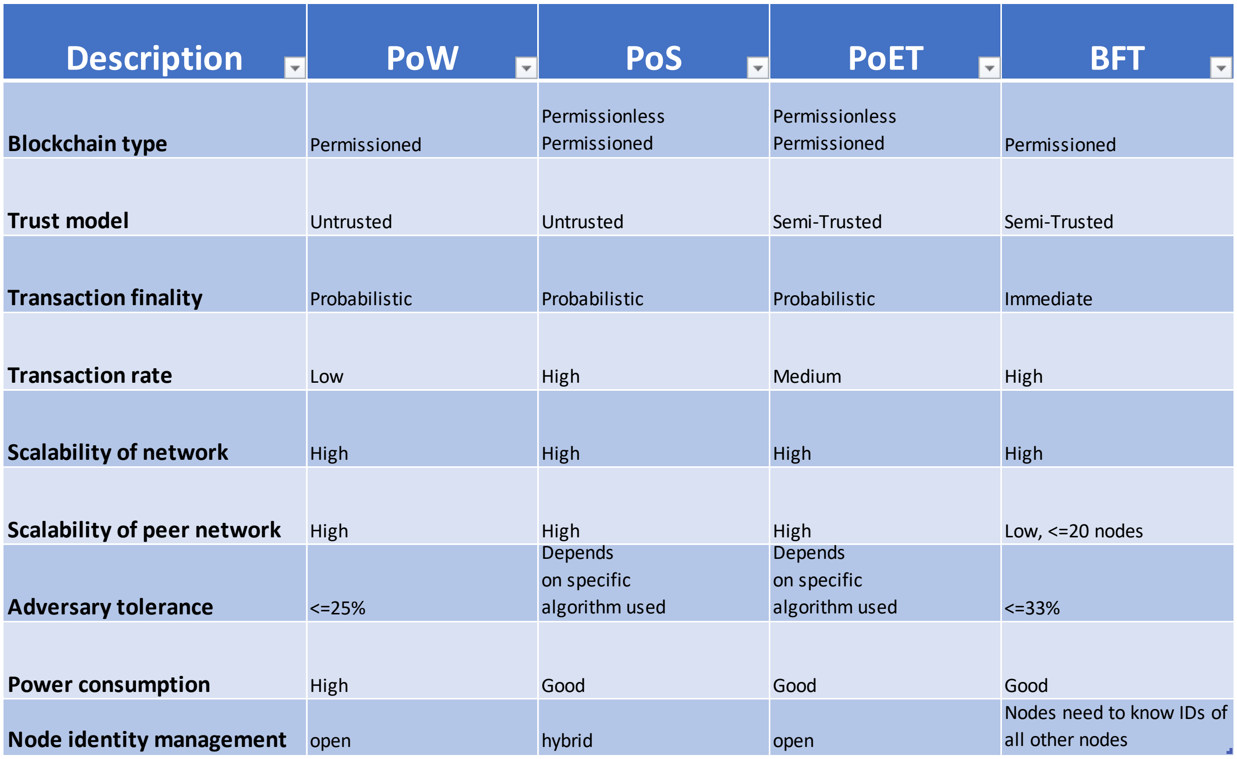
Figure 4 – Consensus Models

- Public blockchain networks utilize PoW to validate a new block. The process involves a race to solve a cryptographic puzzle that is progressive more difficult over time requiring more computing capability. The puzzle prevents patterns; thus, historical answers to past puzzles cannot be utilized to predict the answer to a new puzzle. The node that is the winner of race is rewarded by the network and mined the block to be validated by the remaining nodes. PoW is very power-intensive where hashing work consumes from 250-500 Megawatts of electricity, equivalent to that of major city or a small country. PoW is susceptible to manipulation, i.e. falsifying transactions, double-spending, etc., also known as the 51% attack where an entity controls most of the hash power of the network.
- PoS addresses the power-intensity issue of PoW by allowing nodes to stake or gain the right to publish the block based on the amount of the stake. In other words, a stake of 5% should be able to publish 5% of all new blocks. Additionally, PoS also deters the 51% attack by making the monopoly more costly to execute. However, PoS has its criticisms varying from collusion risks to less decentralization, if the number of staked nodes is not sufficiently large enough. By contrast to PoW, PoS offers faster transaction rate and finality.
- BFT or consortium-based consensus is the most widely selected consensus protocol for private or permissioned networks. BFT does not require a high number of nodes to scale the network in comparison to PoW or PoS. BFT requires a designated set of validator nodes to perform checks where the blockchain decides the next block by allowing participating validators to "vote" on which submitted block to include next.

The design allows for a generalized quorum to be established and tolerates f-out-of-n faulty/adversarial nodes. Hyperledger Fabric utilizes BFT as the consensus model for the endorsing peer nodes where a required quorum of endorsers is mandatory before the transaction is committed.

- PoET is designed to be executed by autonomous nodes where participants wait for the randomly chosen time from a hardware enclave (e.g., a trusted and secure feature available on some hardware), and the network selects a winner based on the shortest wait time. PoET can be built based on Intel's Secure Guard Extensions to provide protection to select code and data from disclosure and modification. PoET is ideal for permissioned and private blockchains in performance and scale.

A technical summary of the four consensus models is shown in Figure 4.



Description	PoW	PoS	PoET	BFT
Blockchain type	Permissioned	Permissionless Permissioned	Permissionless Permissioned	Permissioned
Trust model	Untrusted	Untrusted	Semi-Trusted	Semi-Trusted
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate
Transaction rate	Low	High	Medium	High
Scalability of network	High	High	High	High
Scalability of peer network	High	High	High	Low, <=20 nodes
Adversary tolerance	<=25%	Depends on specific algorithm used	Depends on specific algorithm used	<=33%
Power consumption	High	Good	Good	Good
Node identity management	open	hybrid	open	Nodes need to know IDs of all other nodes

Table 1 – Technical Summary of Consensus Models

Business Logics

4. Business Logic typically exists with 2nd generation (e.g., Ethereum, Corda, Hyperledger Fabric) and 3rd generation (Cardano) blockchain platforms, and the smart contract is engine that executes the business logic. When deployed to a blockchain, the smart contract will lie dormant until it is called by a transaction for the automated execution of logics that support, verify or enforce the performance of a smart contract. The smart contract is immutable, and the business logics cannot be altered once deployed. A smart contract has other unique characteristics that are not discussed in this white paper, but it is important to understand that a smart contract can perform calculations, store information onto the shared ledger, and automatically trigger other smart contracts and APIs (frontend/backend applications, external oracles, data sources). Typically, users interact with blockchain-enabled applications, dApps, as shown below:

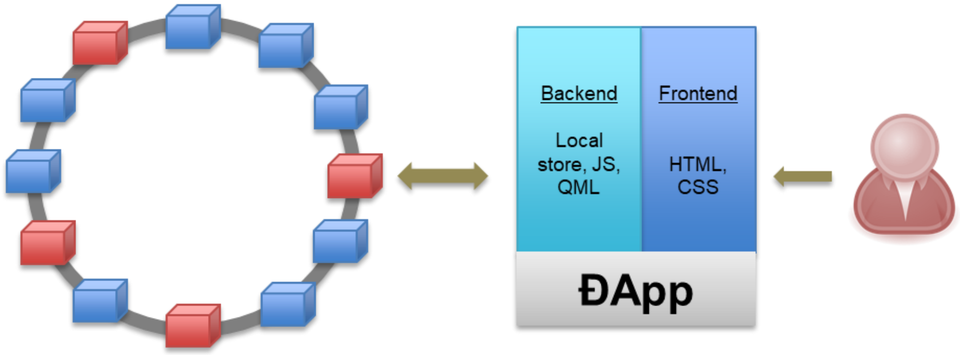
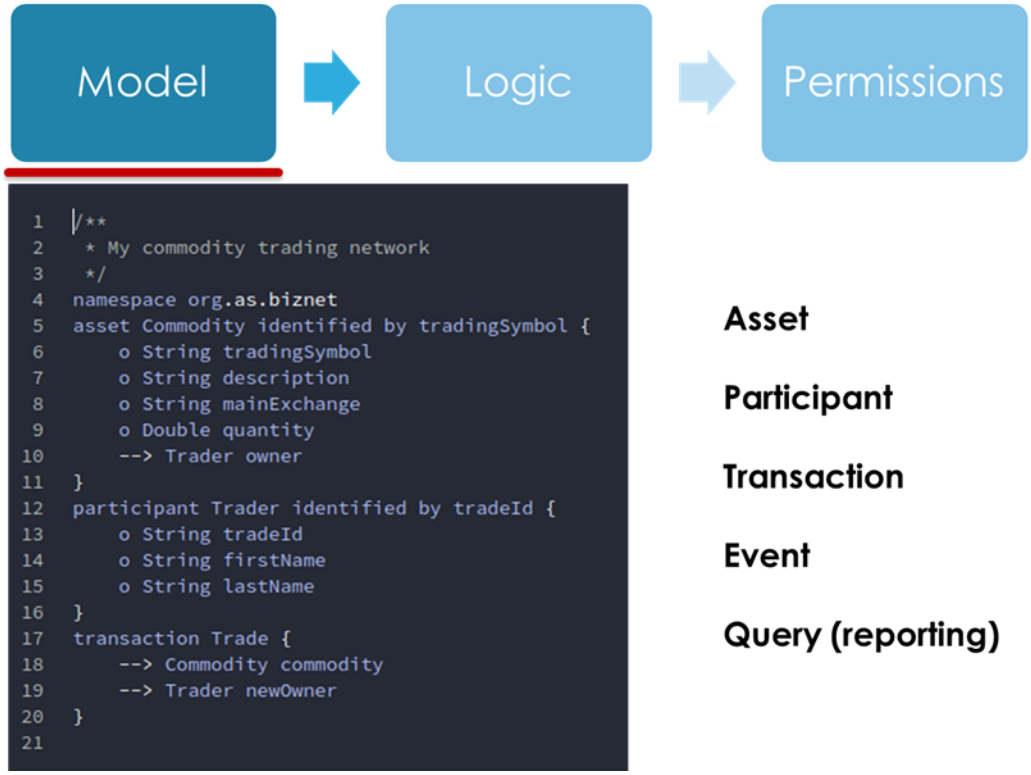


Figure 5 – dApps and Smart Contracts

The use of smart contracts on the blockchain enables the development of new applications enabling people to sell products and services, exchange shares, money, and documents, and maintain origin and shipping manifests of commodities and products, etc. Smart contracts can vary from simple cryptocurrency coin payment to highly complex implementation such as insurance policies, digital publishing rights and logistics management or sourcing/tracking of commodities and assembled products across the various suppliers. While providing significant efficiencies and cost reduction to existing processes, smart contracts have also become a major source of vulnerabilities to be exploit on many blockchain platforms and have resulted in financial loss exceeding $4B in the first two quarters of 2019 alone.

A smart contract (based on Hyperledger) typically requires three key components as follows:

- o Model – Defines the asset, participant, transaction, event and queries to be acted upon.

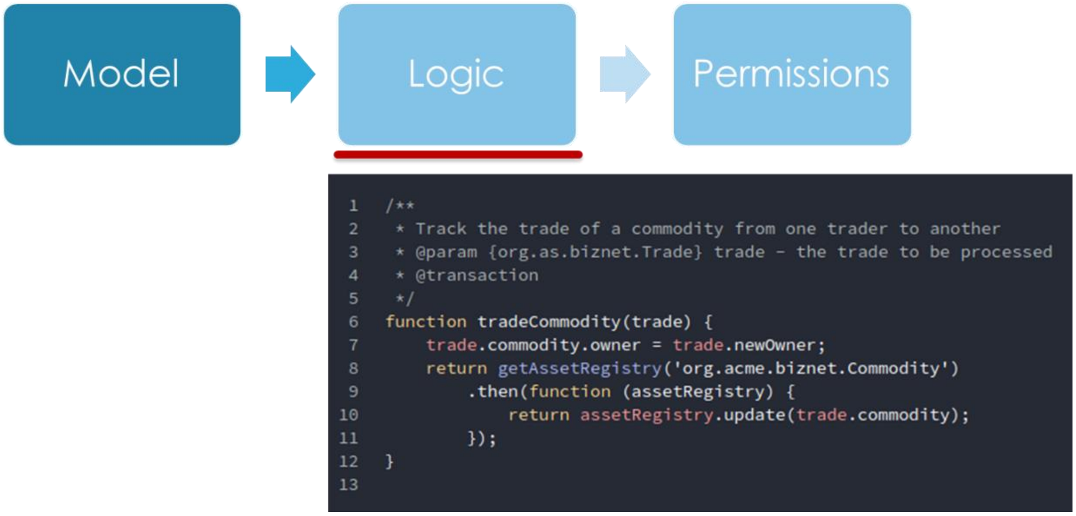


```
/**
 * My commodity trading network
 */
namespace org.as.biznet
asset Commodity identified by tradingSymbol {
    o String tradingSymbol
    o String description
    o String mainExchange
    o Double quantity
    --> Trader owner
}
participant Trader identified by tradeId {
    o String tradeId
    o String firstName
    o String lastName
}
transaction Trade {
    --> Commodity commodity
    --> Trader newOwner
}

```

Figure 6 – Example of a Notional Model of a Network in Hyperledger Fabric

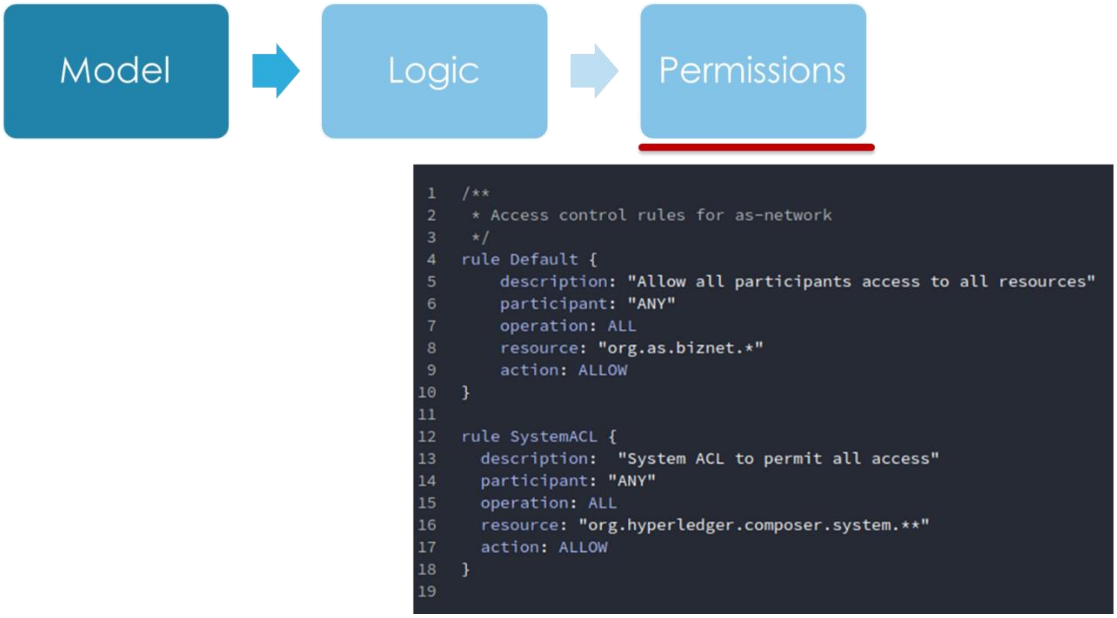
- o Logic – Defines the outcome and relationship between assets and transactions and participants. It is embedded in the ledger design and executed together with transactions, accessible through platform's programming languages such as Go (Hyperledger Fabric) and Solidity (Ethereum).



```
/**
 * Track the trade of a commodity from one trader to another
 * @param {org.as.biznet.Trade} trade - the trade to be processed
 * @transaction
 */
function tradeCommodity(trade) {
    trade.commodity.owner = trade.newOwner;
    return getAssetRegistry('org.acme.biznet.Commodity')
        .then(function (assetRegistry) {
            return assetRegistry.update(trade.commodity);
        });
}
```

Figure 7 - Example of a Smart Contract in Hyperledger Fabric

- Permissions – Controls what the participants can and cannot do within the network, and who controls the smart contract and related contract value.



```
/**
 * Access control rules for as-network
 */
rule Default {
    description: "Allow all participants access to all resources"
    participant: "ANY"
    operation: ALL
    resource: "org.as.biznet.*"
    action: ALLOW
}

rule SystemACL {
  description:  "System ACL to permit all access"
  participant: "ANY"
  operation: ALL
  resource: "org.hyperledger.composer.system.**"
  action: ALLOW
}
```

Figure 8 – Example of Permissions in Hyperledger Fabric

Summary

We are still at the beginning of the blockchain revolution. We discussed that blockchain solutions seek will likely displace traditional services across a variety of industries through efficiency and lower costs. For the financial institutions, we highlighted several specific use cases where blockchain technology has started to reshape the way financial services are structured, provisioned and consumed. We provided patterns to assist organizations to better understanding if blockchain technology may be a good fit for a proposed application or project.

We covered key concepts of blockchain in details to provide the minimum background understanding required in applying the technology. While blockchain technology may be complex and technical to implement, it potentially offers significant improvements to existing processes and methods. In other words, blockchain technology can and have created new business models and corresponding opportunities. However, blockchain technology is not a panacea to solve or improve existing processes, and therefore, organizations need to understand what their true needs are before embarking on the adoption of blockchain technology.

In Part 2 of the Playbook we will dive in the constraints and limitation of blockchain technology and how to avoid the pitfalls of blockchain implementation.

Caplock Security and its partners thank you for your time and ongoing support. We welcome your feedbacks on our Blockchain Technology Playbook.

Tuan Phan, CISSP, CBSP, PMP, Security+, SSBB, is a partner with Caplock Security LLC, where he also serves the practice leader for blockchain technology. He is leading the development of several proofs of concept using Hyperledger Fabric and Ethereum private blockchains and implementing security audits of blockchain technology. Tuan can be reached at 202-780-5455 or tphan@caplocksecurity.com.