W3C Blockchain Use Cases

Editors: Manu Sporny, Marta Piekarska

Contributors: Wayne Vaughan, Daniele Levi, Clint Carlson, Harsh Patel, Boaz Sender, Colleen Kirtland, Adam Lake …

Abstract

A blockchain is a … distributed, append-only database hardened against tampering and revision that provides a single shared source of cryptographically verifiable truth. The use cases outlined here are provided in order to make progress toward possible future standardization and interoperability of blockchains. The use cases in this document focus on concrete scenarios that the technology defined by the group should address.

Table of Contents

Introduction

A blockchain is a distributed, append-only database hardened against tampering and revision that provides a single shared source of cryptographically verifiable truth. The use cases outlined here are provided in order to make progress toward possible future standardization and interoperability of blockchains and ledgers. The use cases in this document focus on concrete scenarios that the technology defined by the group should address.

The W3C Blockchain Community Group at the W3C is investigating the requirements around blockchains and decentralized ledgers. The goal of the Community Group is to determine if there is a sufficient understanding and need to merit the creation of a W3C Working Group to develop Recommendations in this space.

Use Case Model

This document presents an aggregate use case model, comprised of Needs, Roles, Tasks, Sequences, and Interactions. Taken together, these models define the use cases that the Blockchain Community Group will address. For a bird's eye visualization of the use case model, please see (future link insert).

The basic structure of the model contains 5 levels that enable cross industry, sector and domain collaboration.

Level 1	Describes user needs based on key Blockchain characteristics
Level 2	Defines common needs that form an architectural backbone for various Sectors and Domains. These common needs are likely to be shared across industries, sectors, and domains
Level 3	Defines Vertical Sectors, likely to align to industry classification. These sectors have been sourced from various governmental agencies around the world such as the Bureau of Labor statistics. (Example: Financial)

Level 4	Defines Sub Domains that belong to a sector. (Ex. Mutual Funds, Insurance)
Level 5	Encapsulates a group of use cases that may require further analysis/exploration

User needs define the problem space that Blockchains and Decentralized Ledgers address. User Roles specify the roles different entities play when interacting with Blockchains. Tasks define the functions users can accomplish and sequences demonstrate how tasks might be realized by interactions between entities over time.

As with all models, this use case model is neither exhaustive nor complete. The listed uses cannot exhaustively capture all possible use cases. Similarly, the models do not completely characterize the use cases represented. However, the combined model provides specific, coherent guidance for the work ahead.

Terminology

blockchain

> a distributed network, append-only database hardened against tampering and revision that provides a single shared source of cryptographically verifiable truth.
>
> More specifically, it is a software defined network where where the network state and the state of all network entities is cryptographically verifiable. Network state is periodically reached through a consensus mechanism and recorded in a distributed append-only database. The economic incentives to persist the network and the cost of attacking the network must exceed a threshold that provides participants with a strong guarantee of the network's integrity.

sidechain

> …

permissioned

> …

permission-less

> …

NOTE

The Blockchain Community Group recognizes that there are many correct definitions for the term **blockchain**, but for the purposes of this document, we have chosen to use the definition above as it garnered the most consensus.

Ecosystem Roles

There are number of roles supported by blockchains: Archivists, Verifiers, and Node Operators …

Archivist/Writer/Creator/Alice

An entity that requests storage of a piece of information to the blockchain.

Verifier/Auditor

An entity that reads the blockchain in an attempt to ensure the cryptographic soundness of a piece of information stored in the blockchain.

Node Operator/Miner

An entity that places information into a block.

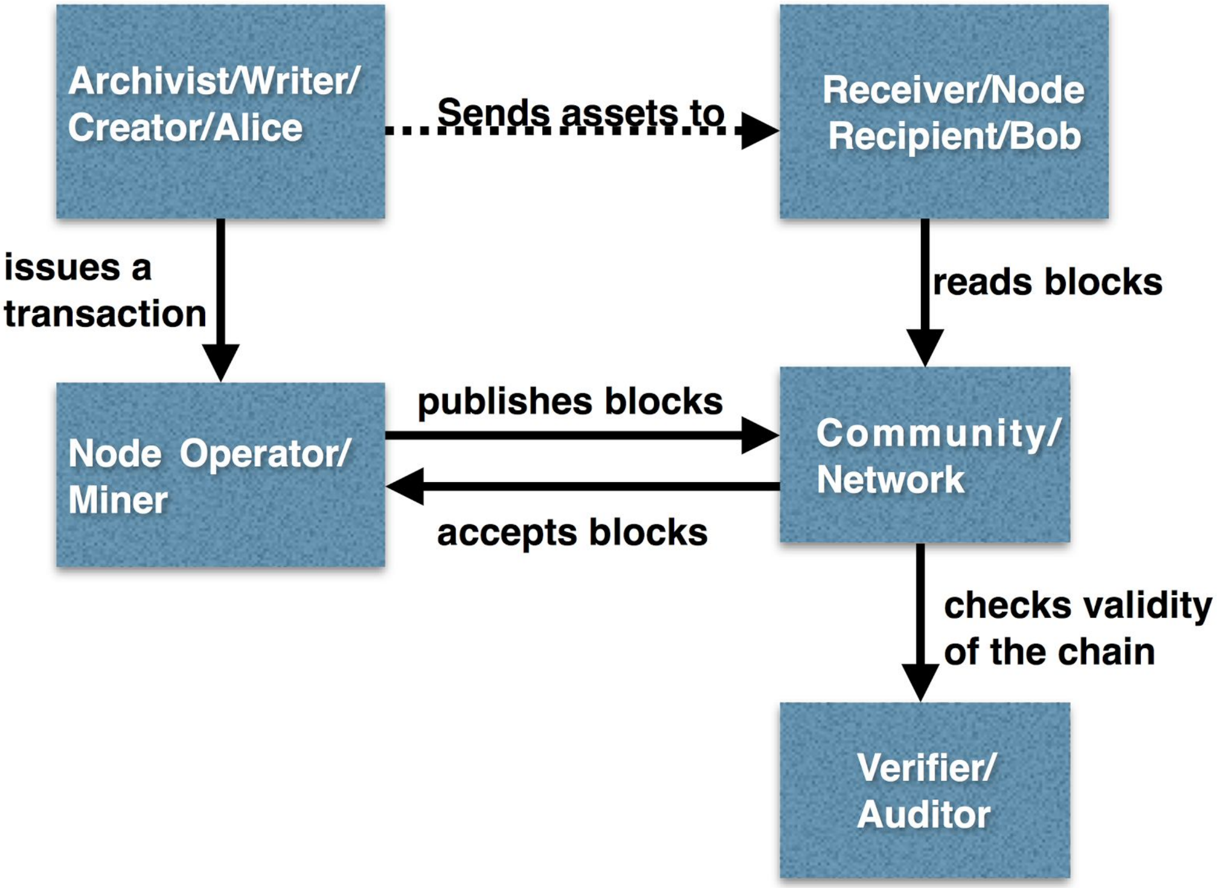
Community/Network

An entity that holds the whole record of blockchains

Receiver/Node Recipient/Bob

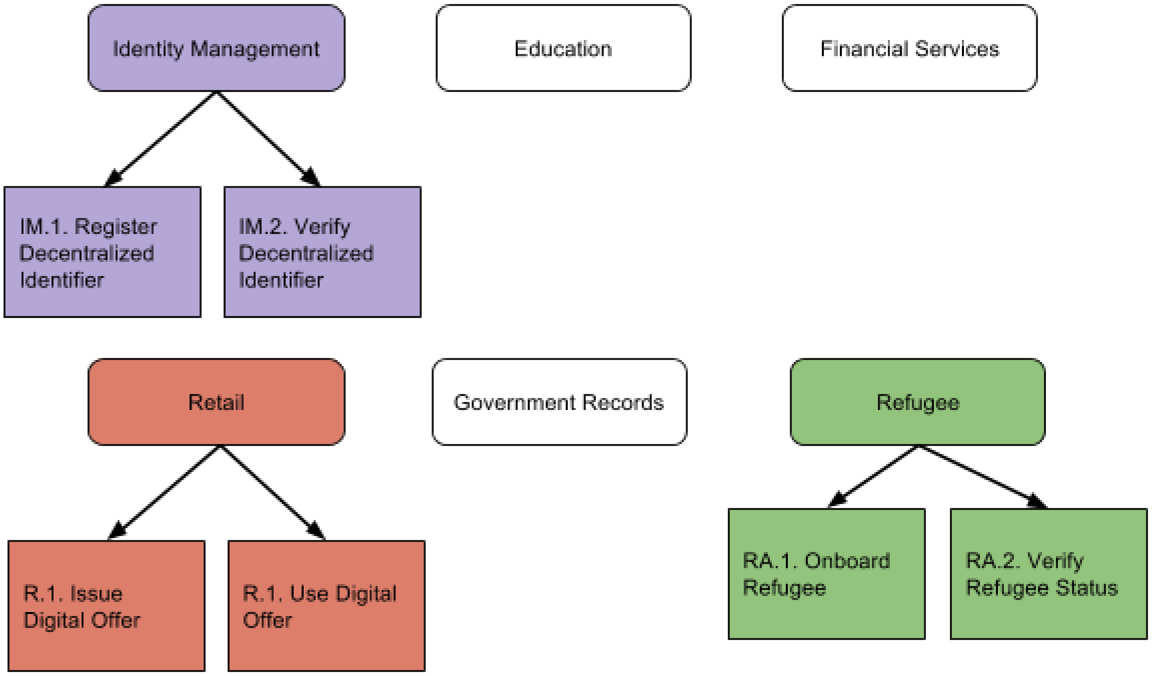
An entity that reads/receives data.

Ecosystem Overview



Domain Needs

Blockchains address user needs in a number of key domains:



Identity Management

IM.1. Self Sovereign Identity

Susan wants to control her identity on the web rather than her identifiers being controlled by another entity. She registers an anonymous identifier that she can solely prove ownership of. This not only gives her single sign-on capabilities to participating websites but digital credentials of any kind, like a drivers, can be issued to the identifier that only Susan controls.

Education

E.1. Credential Revocation

A teacher certification is issued to a particular person by an an educational institution. Teachers are required to fulfill periodic testing requirements to maintain their teacher certification. If these requirements are not met the educational institution can write the revocation of the teacher’s certification to a revocation ledger(a.k.a bockchain). When teacher certifications are inspected the revocation ledger is queried to verify that the teacher certification is up to date.

E.2 Certification Validation

Authenticating education credentials.

Financial Services

TBD…

F.1. Exchange Traded Funds (hidden trade volume or other meta)

F.2 Currency Exchange

Healthcare

Healthcare is a vast and complex industry consisting of, but not limited to, the following entities: hospitals/clinics, insurance companie, patients, physicians, nurses, and pharmacies.

H.1. Certification Revocation

Barney is a physician, and has recently become board certified in his state. The state's board issues Barney a digital certificate confirming that he is certified to practice medicine in that state. Barney can now use this certificate, until the expiration date of the certification, when writing prescriptions and referrals, thereby improving accountability and verifiability. However, if Barney's certification were to be revoked as a result of some misconduct the digital certificate will still be valid. To address this, a blockchain is created by a consortium of the 24 boards that certify physician specialists in the United States as well as any other stakeholder who should have the right to revoke a doctor's certification. Any of these consortium members can write the revocation of Barney's digital certification to the ledger. When verifying the credential the pharmacy inspects the Barney's credential as well as queries the revocation ledger to determine if the Barney has the authority to write a prescription. If the the certification is deemed valid and there are no revocations of that certification on the ledger the prescription is deemed valid and filled. If the certification is invalid or there is a revocation of that certification on the ledger the prescription is deemed invalid and not filled.

The digital credential issued to Barney for the purpose of signing a controlled substance prescription must have

Federal (e.g. US Drug Enforcement Agency - DEA) non-repudiation. This implies an auditable link between the identity certification authority (e.g.: State Driver's License or Passport Authority) and the biometrically secured signing technology (e.g.: Blockchain DID) that is used to sign the prescription. In this controlled substance prescribing use-case, as in the real-world DEA case, there are two certification authorities: (a) the medical board certificate controls the identity used to access the prescription writing app and, (b) the DEA controls access to the digital signing certificate used for the prescription. In the most general case, the DEA certificate can be dependent on a valid medical license and automatically revoked if the medical license is revoked.

H.2. Certification Validation

Certiificaiton Validation, reputaion…

H.3. Prescription to patient

Insurance

Fraud in increasing in the insurance industry and currently represent billions of dollars of losses annually.

I.1. Double Spend

George gets auto insurance with a new insurance company, InsuranceX, but accidentally forgets to cancel his old insurance policy with InsuranceY. Before he realizes this error he gets into a minor accident. Realizing that he has two policies, and not necessarily knowing it's illegal, he makes a claim with both insurance companies. However, InsuranceX and InsiranceY have recently joined forces to stop this double spend scenario by creating a shared ledger that each company writes their claims to. If two similar claims filed under the same VIN (vehicle identification number) are filed around the same time, the claims are flagged for further inspection. InsuranceX and InsuranceY compare claims and it's determined that the claims are for the same damage. George's claim is denied.

2. …

…

Government Records

TBD…

Real Estate

TBD…

Land ownership

R.1. Rental Fraud

Freddy Fraudster copies a the information from a real rental listing and posts it on a Real Estate site for rent. Joe, and contacts Freddy who requests that Joe transfers money to Freddy as a “service fee” to prove he is a viable renter before touring the rental in person. Joe, knowing that rental fraud is an issue looks up the rental on a public blockchain to verify that Freddy’s credentials match the owner written to the blockchain. Joe finds out that Freddy is not the true owner of the rental, does not transfer the funds, and avoids the rental scam.

Supply Chain

Supply chain management (SCM), the management of the flow of goods and services, involves the movement and storage of raw materials, of work-in-process inventory, and of finished goods from point of origin to point of consumption.

SC.1. Fair Trade Certification

FairTradeManufacturer claims source ingredients that pay farmers even more than typical fair trade standards. FairTradeManufacturer produces health food products with many ingredients and wants to prove to the end consumer of their higher compensation to farmers. To achieve this they move their supply chain management to a blockchain where ingredient purchases as well as manufacturing details are written to the immutable database for anyone to view. Any customer or third party verifier can view the supply chain records and verify that FairTradeManufactur does indeed pay farmers 50% more than typical fairtrade standards.

Organic Certification

Commodity Tracking

Commodity, particularly international freight shipping, involved many entities and many signed paper documents. This makes the shipping process open

Refugee

The refugee domain includes documentation of identity and tracking of aid.

Rg.1. Identity

HumaNGO collects information about a Refugee and issues them a digital ID that is written to an Identity Blockchain. As a refugee migrates and interacts with other NGO's or governments. Those interactions and documentation be verified later via an identity blockchain. This gives the refugee irrefutable documentation of the timeline of their migration.

Rg.2. Aid Tracking

Aid

Retail

The Retail domain includes online retail, brick and mortar retail, loyalty card providers, consumer packaged goods companies, retail software vendors, coupon providers, distribution, and coupon clearinghouses.

Rt.1. Issue Digital Offer

Yum Cola distributes high value digital offers (50% off) in conjunction with a new brand of cola (Yum Cola Fresh) that they are launching. They would like to make sure these coupons are not used more than once, so they enter each coupon serial code into a coupon blockchain to track their use.

Rt.2. Use Digital Offer

Benny buys a 6-pack of Yum Cola Fresh using the 50% off coupon. The retailer's Point of Sale system: 1) reads the coupon, 2) checks the coupons status on the coupon's blockchain, and 3) if the coupon has not already been marked as used, marks the coupon as used.

Tasks and Requirements

Use cases are often used as a driver for requirements. While the users of DLTs have needs across many domains, the tasks associated with those needs span the domains. This section summarizes those tasks, as well as requirements related to the tasks, and maps the tasks and requirements back to the associated needs.

Store Information

TBD - use cases having to do with storing information in a blockchain.

Replicate/Distribute Information

TBD - use cases having to do with replicating/distributing information and coming to consensus.

Verify Information

TBD - use cases having to do with verifying information in a blockchain.

NEEDS CATEGORIZATION

We may want to integrate these use cases as well:
https://image-store.slidesharecdn.com/bbf93c69-38c2-4e6e-bf98-b20335d70e1d-original.jpeg

6 Categories of Trust around personal data transactions (adrian)

- identifying the person that is the subject of the data,
- identifying the user requesting person's data,
- recording and auditing the authorization to release the person's data,
- establishing the authenticity of the data that is being released,
- paying the service that offered the personal data,
- and auditing that the shared data was used as expected.

Each of these six could be a different blockchain and a different standard.

More use cases:

- for wallets, we want some way to store and operate on keys in a secure way in the client. I believe web crypto is working on this. Will the web crypto group's APIs suffice for wallets? (boazsender)
- for natural disasters/emergency skill systems: running a ledger with no "servers"- distributed networking. Network discovery/management from the browser, or maybe over BLE? (boazsender)
- verify a block is genuine inside a blockchain from a web application (brunoj)
- anonymised deterministic passport real-time status validation on travel (dcosta72)
- (harry) Access to bitcoin wallet securely in the browser for payments

- Standardized REST API for blockchain access using normal JSON (harry)
- hyper system centralized and de-centralized DB(permissioned) (jay)
- rights management, trust management on WEB (jay)
- WOT related BC components (jay)
- Checking to see if a doctor has their license (or has been debarred) (manu)
- Checking to see if an IBAN number has been placed on a government watchlist (manu)
- Ensuring that a refugee that is onboarded at one camp can recover their refugee status determination paperwork. (manu)
- Related to the item right above, could digital identification management system be blockchain-based? (nick)
- Preventing fraud in the insurance industry (by registering insurance claims on a blockchain / shared database) (manu)
- Seeing if a car insurance claim has already been processed (fraud) (manu)
- Seeing if a digital coupon has already been redeemed (coupon fraud) (manu)
- that they say they do (manu) Seeing if someone has the credentials (training/education). Lifelong, cross institutional educational badges (mapping versions 1 and 2 of the Open Badge spec to a smart contract). Similarly for ePortfolios. Supporting peer based accreditation (e.g. in the workplace). (John D)
- standardized data model for expressing primitives off of blockchain (returned when using a REST API) (manu)
- verifying if an emergency responder is currently authorized to be onsite (manu)
- calculating Weighted Centrality (mountie, https://github.com/mountielee/reports/wiki/Weighted-Centrality-of-Ledgers)
- Blockchain use by the Music industry: https://medium.com/cuepoint/how-the-blockchain-can-change-the-music-industry-part-2-c1fa3bdfa848#.m462v6ppa (renato)
- Things communicating within IoT (Marta)
- Tracking data that's shared on the Web, and measure who's accessing it (Marta)
- Clearing and settlement processing of digital ticket related services in passenger transportation service and logistics (Ian Shim)
- Striking a balance between Privacy and legal surveillance along with right to be forgotten (Harsh Patel)
- Putting down legal delimitation for ownership and custodianship of data holded by providers. (Harsh Patel)
- Ensuring public policy reaches grass root and enabling better public services. (Harsh Patel)
- Preventing Fraudulent Insurance Claims

- Smart contract arbitration/mediation protocols (Nick)

List of differentiation between Blockchains

- Permissioned vs. permission-less
- Consensus algorithms
    - Proof of work
    - Proof of stake
    - Hashgraph?
- Smart Contracts or not
    - Ethereum
    - Smart Contracts on Bitcoin
    - Claims of Turing-completeness
- Immutability

Open Questions

The following list of questions are designed to elicit from business users if they should consider using blockchain technology.

Do you need:

1. Transactions that are irrevocable? (Transactions that can be proven to be irreversible?)
2. Transactions that where we need to prove that nothing was altered?
3. Where everyone who is a part of a "community" or block can see what has transpired?
4. Where we need to track tangible or intangible items/assets?
5. Where we want to drastically reduce the number of "middle men" and toll gates required in a current transaction?
6. Where there is a fixed pool of assets/objects that we want to ensure are not "spent" twice?
7. Where we want to transcend the jurisdictions of geography when transacting?
8. Where we care about highly secured methods of transacting?

User Sequences

The transaction examples in this section describe basic ways in which DLTs might be used. They are not meant to be architecturally constraining. Instead, they are meant to help illustrate the basic way it *could* be done in a typical interaction. Again - please remember that it is just an example, and should not be thought of as the canonical way such an DLT environment must be implemented.

Specific Real World Examples

Interaction models describe a complete story where only part of the story is applicable to the User Tasks or User Sequences in this document. They help paint a picture of the sort of environment that DLT technology will operate within.

- https://github.com/mountielee/reports/wiki/Blockchain-(Real-world)-UseCases
- Measurement for the information exposed (Youngwan volunteers Vicki)