W3C Blockchain Use Cases

Editors: Manu Sporny, Marta Piekarska

Contributors: Wayne Vaughan, Daniele Levi, Clint Carlson, Harsh Patel, Boaz Sender, …

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.

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.

User 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

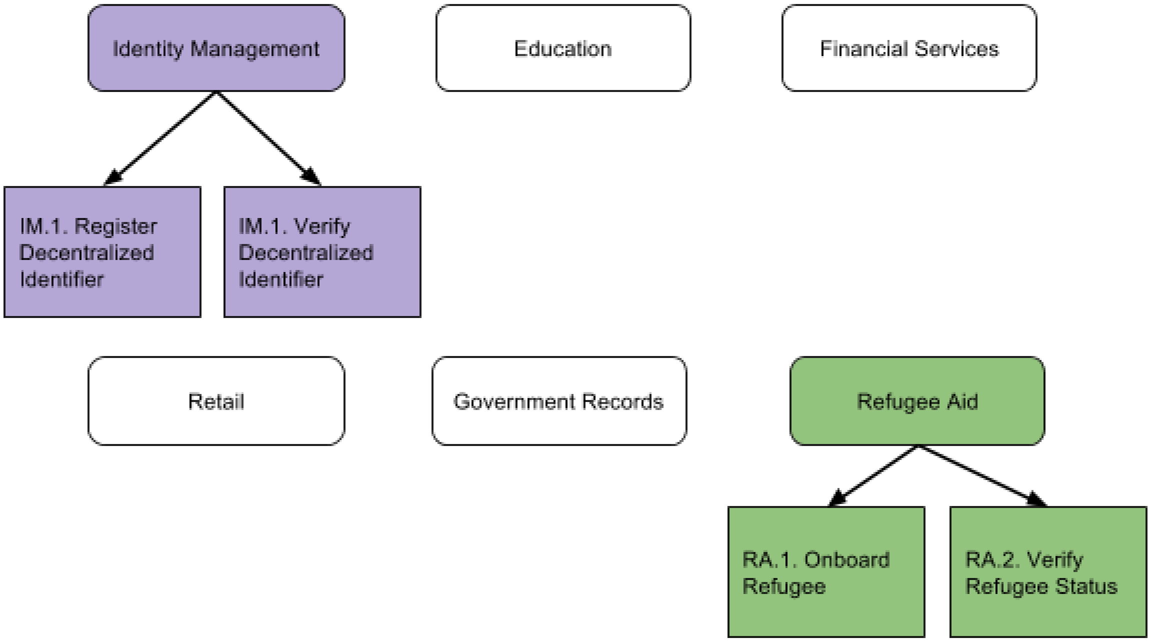
An entity that holds the whole record of blockchains

Receiver/Node Recipient/Bob

An entity that reads/receives data.

Domain Needs

Blockchains address user needs in a number of key domains:


Identity Management
Education
Financial Services
IM.1. Register Decentralized Identifier
IM.1. Verify Decentralized Identifier
Retail
Government Records
Refugee Aid
RA.1. Onboard Refugee
RA.2. Verify Refugee Status

Identity Management

TBD…

Education

TBD…

Financial Services

TBD…

Healthcare

TBD…

Government Records

TBD…

Real Estate

TBD…

Refugee Aid

TBD…

Retail

TBD…

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.

Distribute Information

TBD - use cases having to do with 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)
- 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

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

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 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