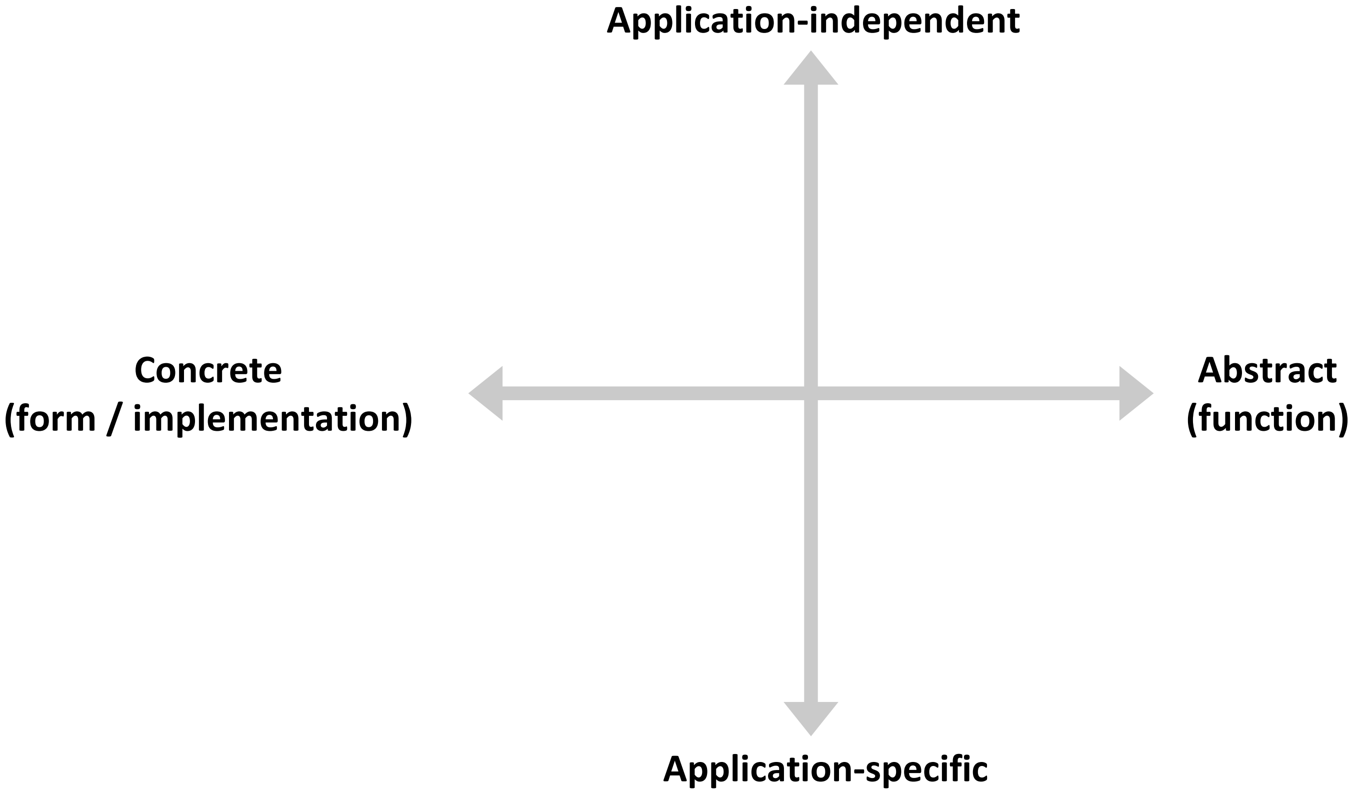
Blockchain Definition and Foundational Building Blocks

David Tennenhouse <dtennenhouse@vmware.com>
Brian Behlendorf <brian@behlendorf.com>

Our questions:

1. What is an overarching blockchain definition that can be used to advance community/legislative discussions? (consider other states and federal definitions to reach alignment counties/states/global systems)
2. How can the context of an application be incorporated to the blockchain definition to highlight different aspects of blockchain?
3. What components of blockchain should be highlighted? How should these components be incorporated into a decision making and an assessment process to determine blockchain technology appropriateness for any use case?
4. Consider the consequences of too narrow or too broad of a definition to ensure that we forge an adaptive path forward for blockchain implementation in California. Consider implication beyond this legislation.

Approach to definition



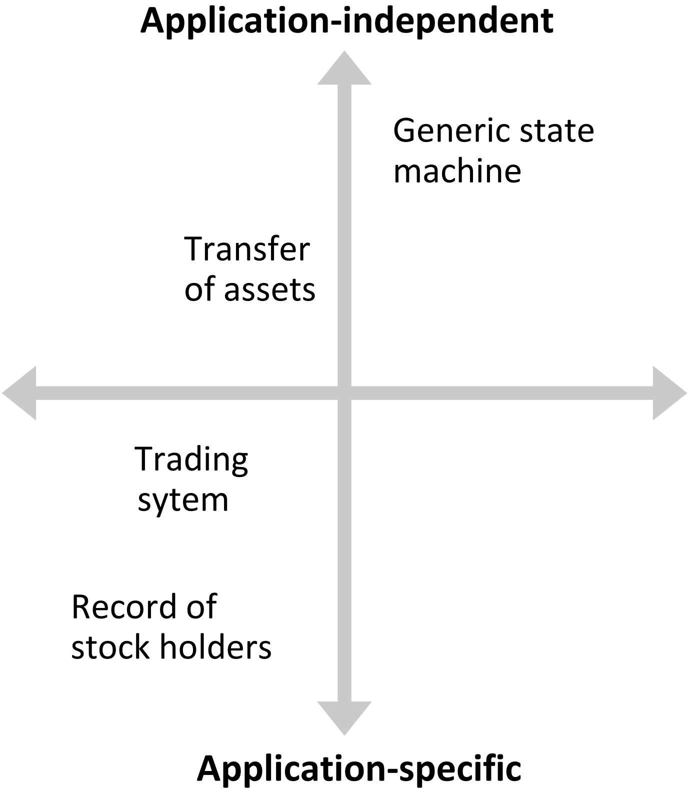
Application-independent

Concrete (form / implementation)

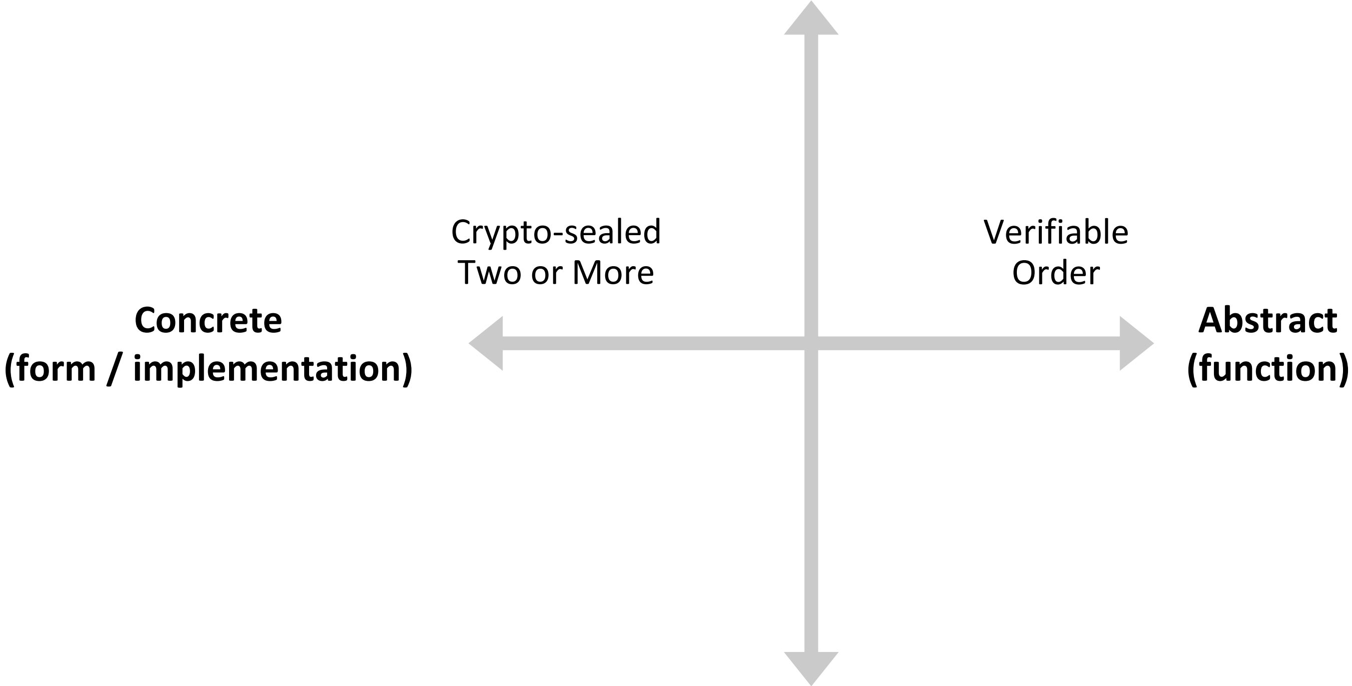
Abstract (function)

Application-specific

Example:


Application-independent
Generic state machine
Transfer of assets
Trading sytem
Record of stock holders
Application-specific

Example:



Crypto-sealed
Two or More

Verifiable
Order

Concrete
(form / implementation)

Abstract
(function)

We looked at vocabulary and phrases used by some other states

(not an exhaustive survey)

Datastore vocabulary

- Datastore / Record / Log / Ledger of Inputs/Actions
- Decentralized / Distributed / shared / replicated
- Uniformly ordered / Consistency / Chronological

  State Machine Replication, finalized, etc.
- Immutable / Auditable / Reproduceable / Non-repudiation

  Retrievable and reproducible in paper form (applies to specific records)
- Mathematically verified / Validated by use of crypto / Crypto-Sealed / Crypto-secured

  Method to verify and store record(s) secured by the crypto hash of previous transaction info
- Blocks
- Data address

  String of chars only accessible using a private key to facilitate or record transactions (also used for identity and signatures)

Smart contracts and token vocabulary

- Contract stored as a record than can be verified by a blockchain
- Event driven program with state / runs on xxx ledger / can take custody (instruct) transfer of assets on ledger
- Tokens – capable of being traded w/o an intermediary
- Tracking tangible/intangible assets

Governance vocabulary

- Public / Private
- Permission / Permissionless
- Unaffiliated parties
- Redundantly maintained by 2 or more…
- Tokenized crypto economics, rewards
- Uncensored
- Visibility into and ability to validate and/or change state of datastore

…with an eye to retaining the concepts most generic and essential to blockchain function …while avoiding those that appeared prescriptive wrt application or implementation

Datastore vocabulary

- **Datastore** ~~/ Record~~ / Log ~~/~~ **Ledger** ~~of Inputs/~~**Actions**
- **Decentralized** ~~/ Distributed /~~ **shared** ~~/ replicated~~
- Uniformly **ordered** / Consistency / ~~Chronological~~

  ~~State Machine Replication, finalized, etc.~~
- ~~Immutable~~ / Auditable / Reproduceable / Non-repudiation

  ~~Retrievable and reproducible in paper form (applies to specific records)~~
- ~~Mathematically verified / Validated by use of crypto / Crypto-Sealed / Crypto-secured~~

  ~~Method to verify and store record(s) secured by the crypto hash of previous transaction info~~
- ~~Blocks~~
- ~~Data address~~

  ~~String of chars only accessible using a private key to facilitate or record transactions (also used for identity and signatures)~~

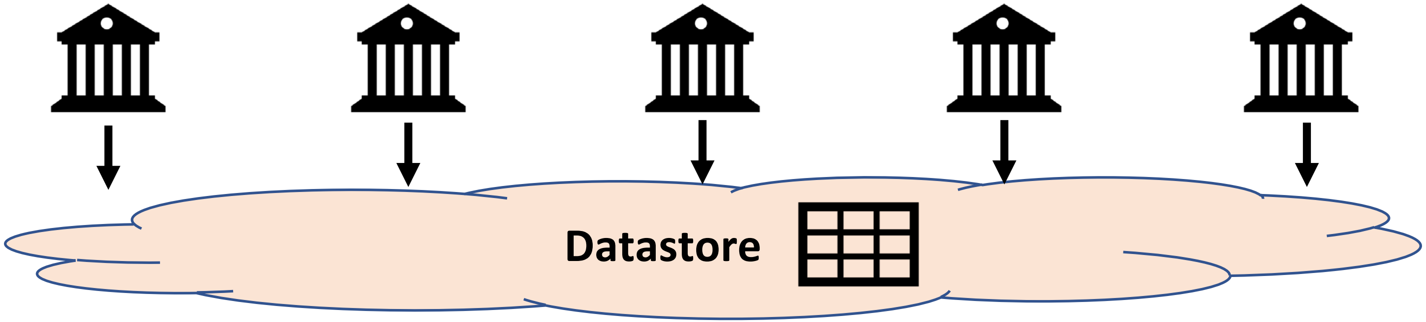
Smart contracts and token vocabulary

- Contract stored as a record than can be verified by a blockchain
- ~~Event driven program with state / runs on xxx ledger / can take custody (instruct) transfer of assets on ledger~~
- ~~Tokens – capable of being traded w/o an intermediary~~
- ~~Tracking tangible/intangible assets~~

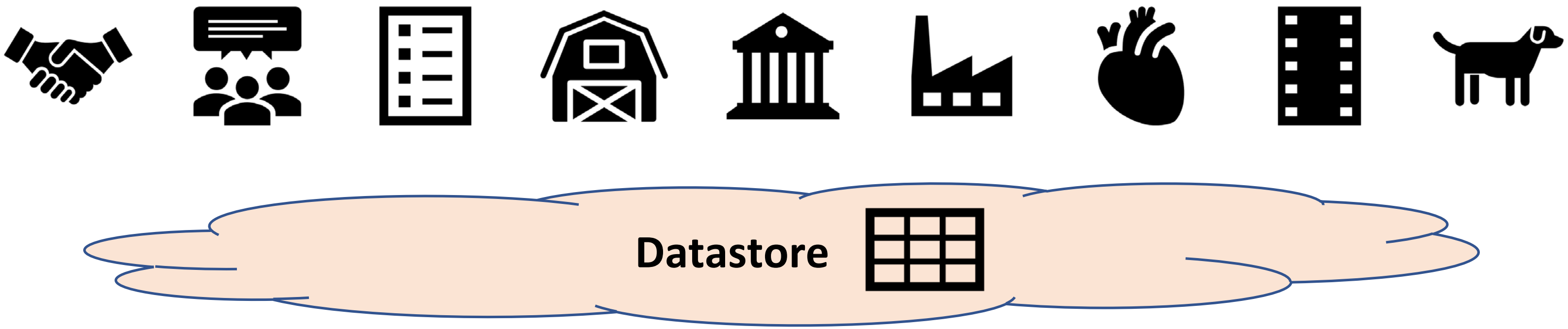
Governance vocabulary

- ~~Public / Private~~
- ~~Permission / Permissionless~~
- ~~Unaffiliated parties~~
- ~~Redundantly maintained by 2 or more…~~
- ~~Tokenized crypto economics, rewards~~
- ~~Uncensored~~
- ~~Visibility into and ability to validate and/or change state of datastore~~

Datastore:
verifiability of data shared amongst participants

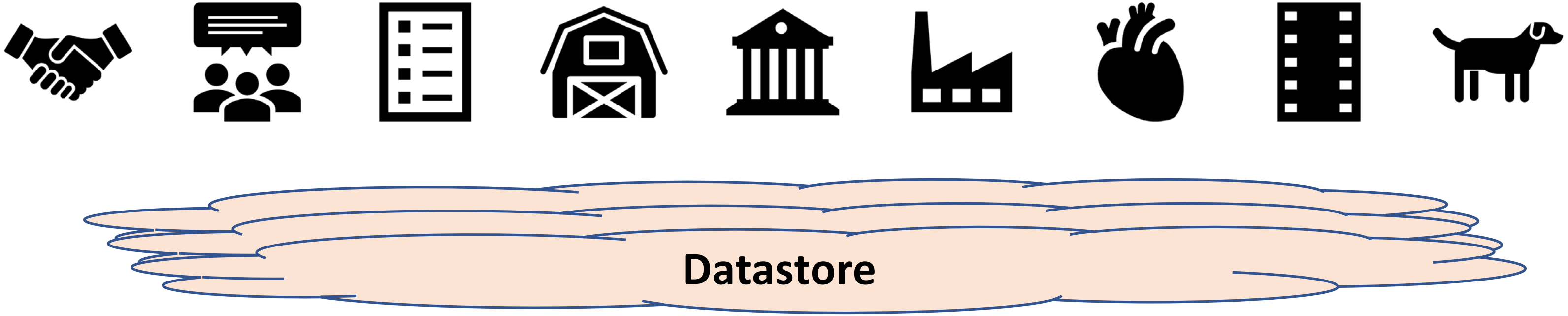


Datastore can be used by many types of participants / applications



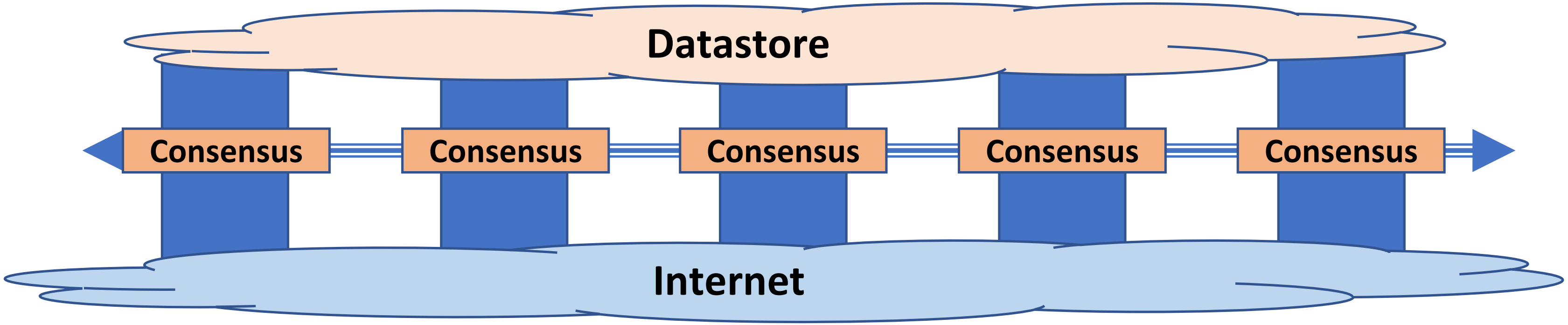
Datastore

There can also be many datastores

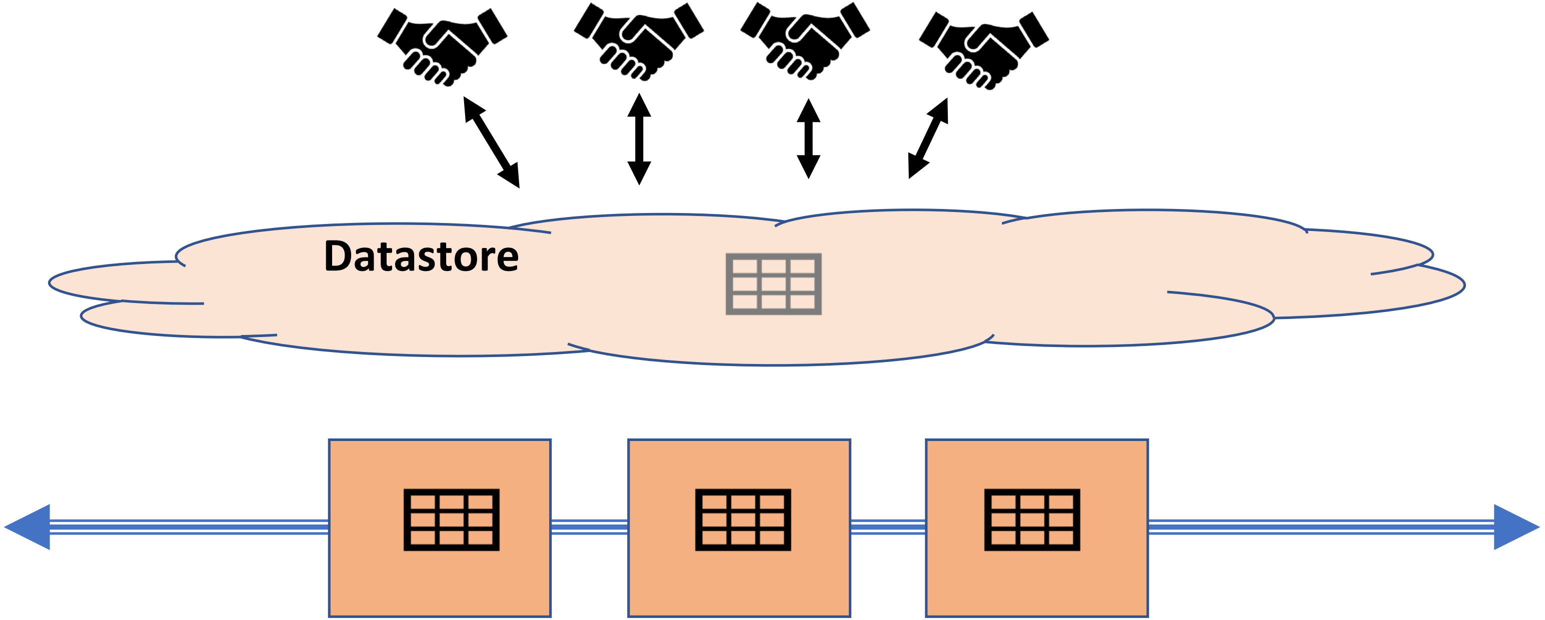


Datastore

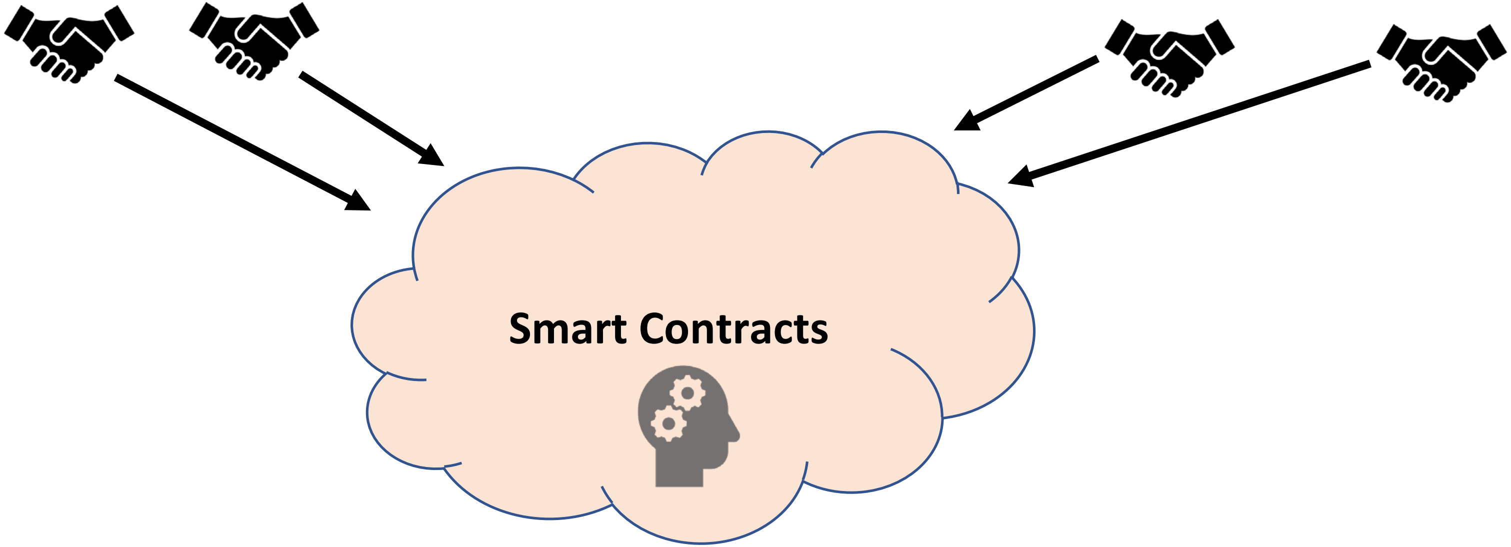
A consensus mechanism is typically used to ensure the *verifiable ordering* of *transactions* (changes to the datastore)



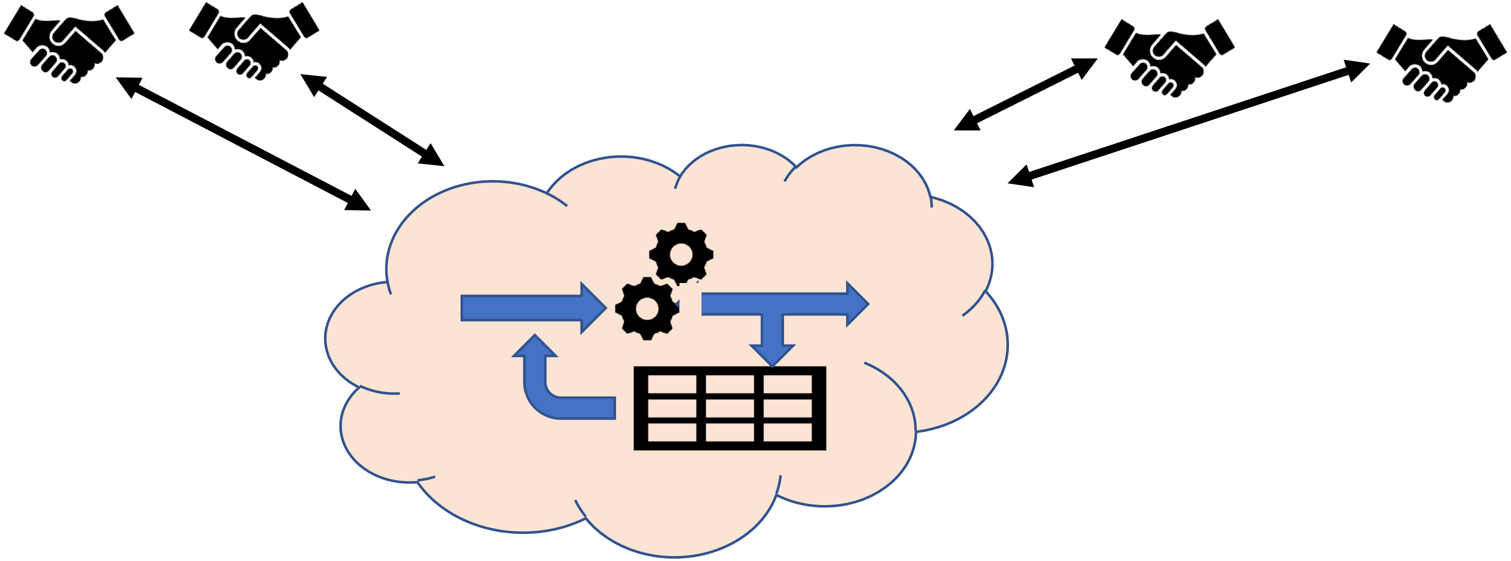
…the nodes of the consensus layer cooperate to maintain the verifiable ordering of transactions



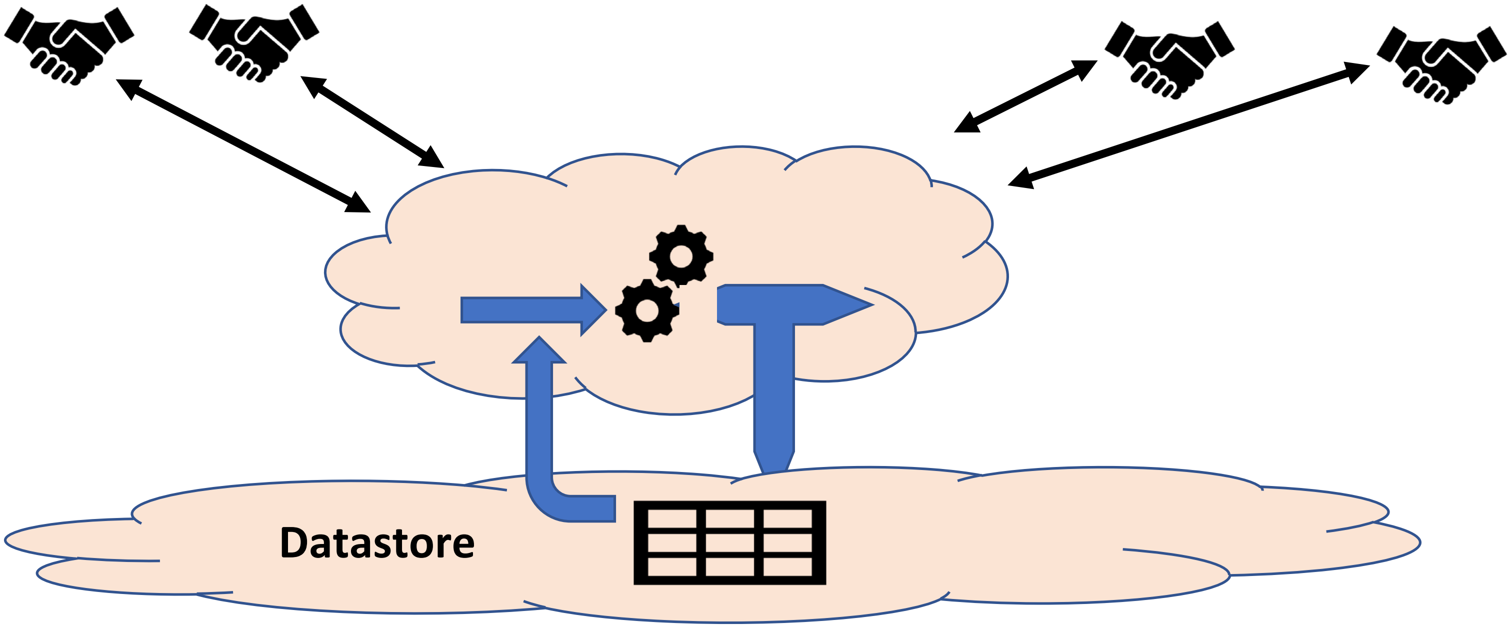
Smart contracts:
Allow participants to automate pre-agreed business processes



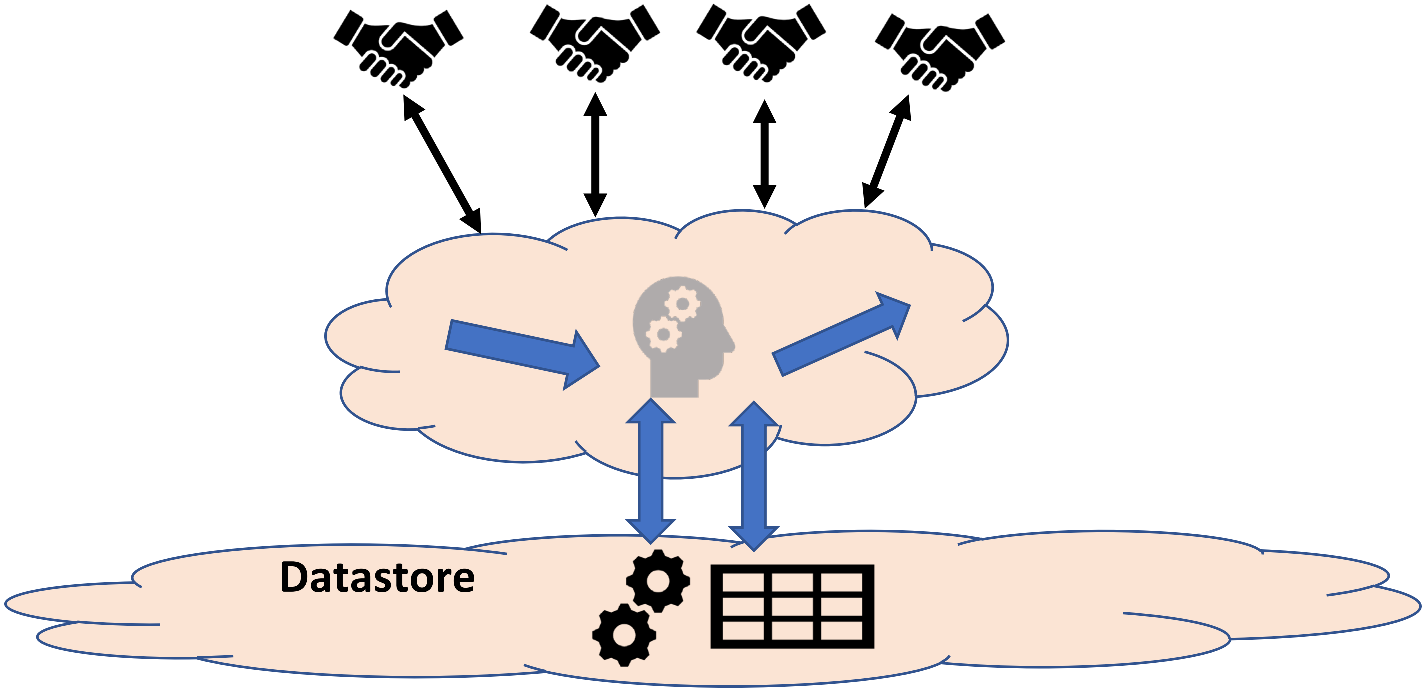
Smart Contract Mechanism: *Rules* & *State*



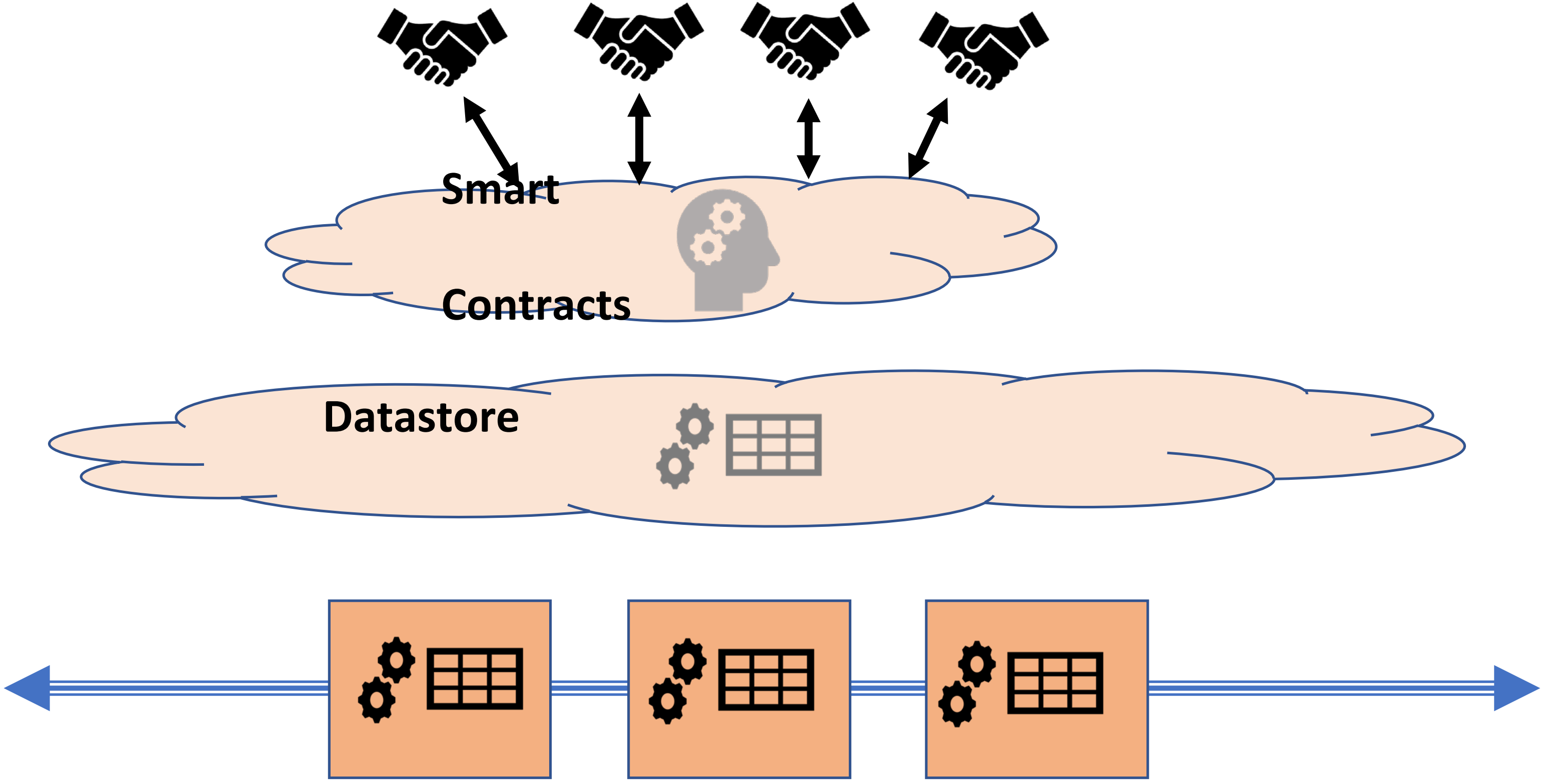
Contract *state* can be kept in the datastore



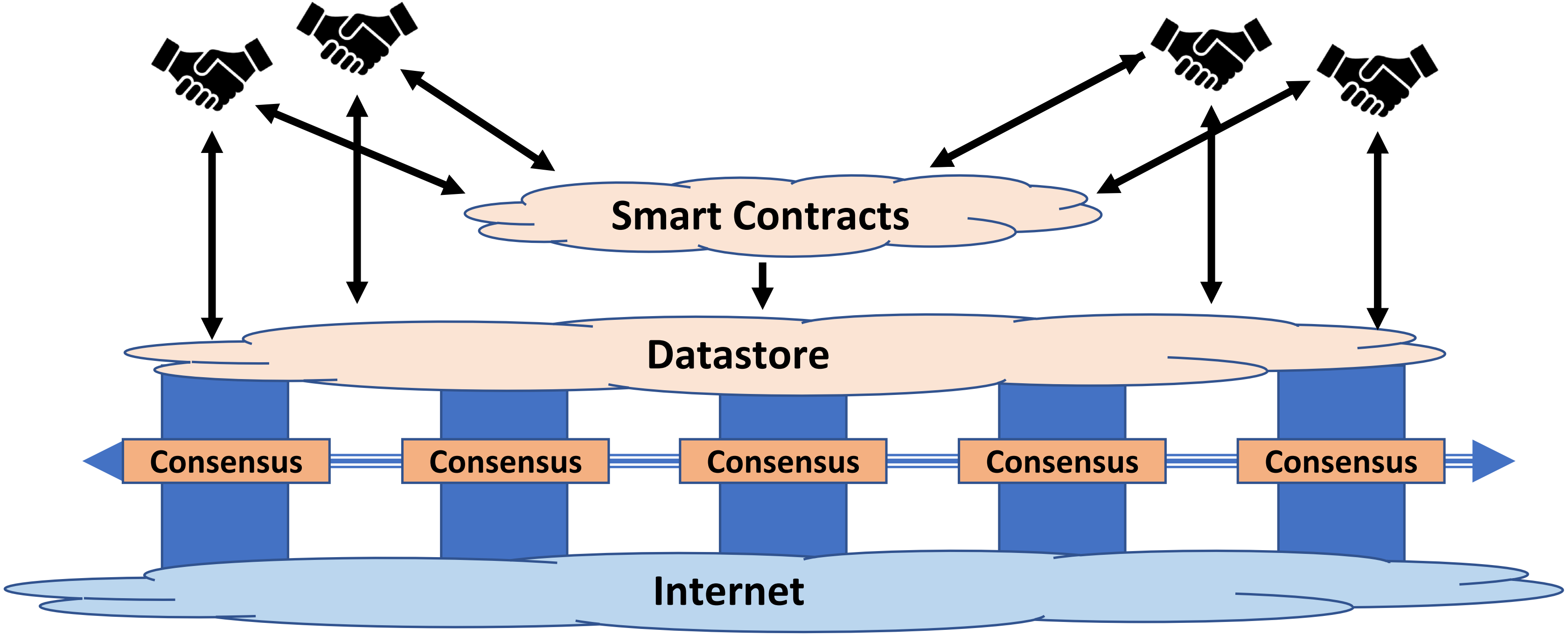
Contract *rules* can also be kept in the datastore!



…with the verifiable ordering implemented by a consensus layer



Putting it all together…



Our Proposed Definition

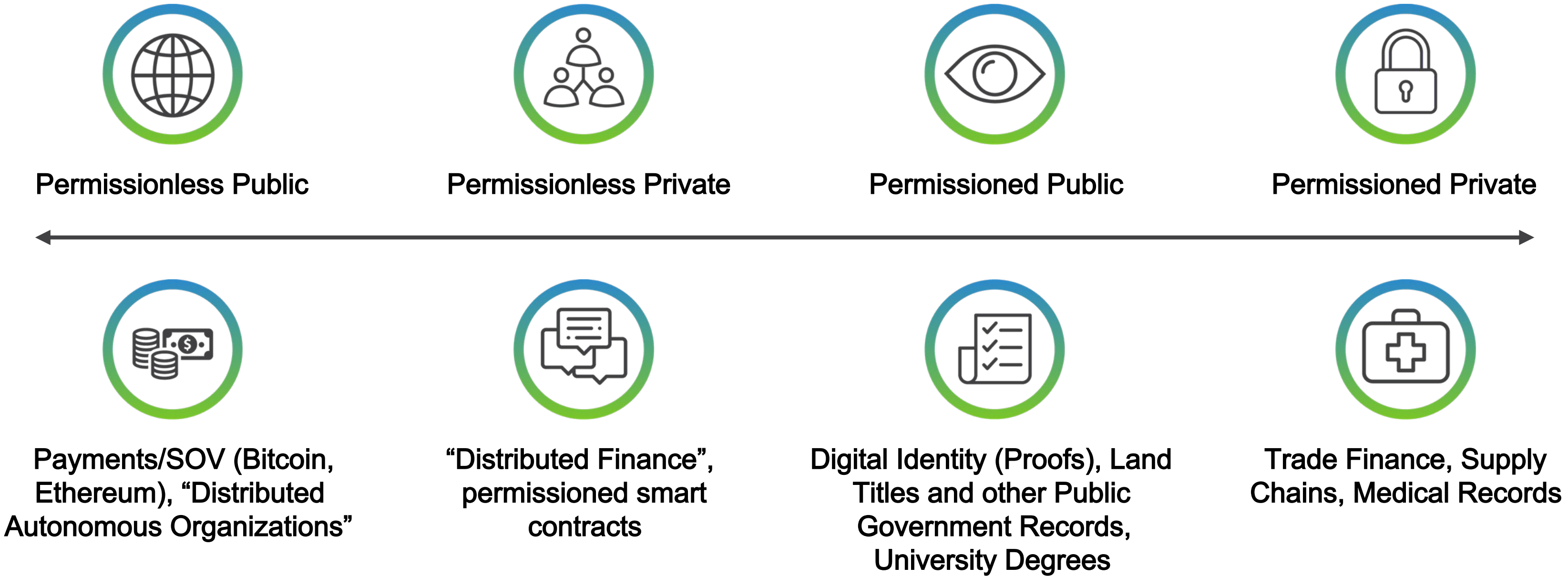
Blockchain technology is used to build decentralized systems that increase the verifiability of data shared amongst a group of participants, which brings increased trust to the overall system.

This definition includes specialized datastores, sometimes called “distributed ledgers”, that provide a verifiable ordering of transactions on the datastore.

This definition also includes “smart contracts”, which allow participants to automate pre-agreed business processes, which are implemented by the system as a whole through transactions on the datastore.

Permissioned vs. Permissionless: Who can write to a Blockchain (participation)
Public vs. Private: Who can read from a Blockchain (visibility)

There is a role for government, either as publisher or regulator, in all of these.



Permissionless Public	Permissionless Private	Permissioned Public	Permissioned Private
Payments/SOV (Bitcoin, Ethereum), "Distributed Autonomous Organizations"	"Distributed Finance", permissioned smart contracts	Digital Identity (Proofs), Land Titles and other Public Government Records, University Degrees	Trade Finance, Supply Chains, Medical Records

An Adaptive Path Forward?

Legislation / Regulation:

- Focus on the function rather than its implementation.
- Be a stakeholder in governance models – not the governing body itself.
- Reinvent role of regulator as a standards-setting consumer/adopter.

As a Consumer/Adopter:

- Establish center of competency/excellence to guide projects and procurement criteria/selection (i.e. be a smart buyer).
- Avoid vendor capture and lock-in at all levels.